

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«До захисту допущено»

Завідувач кафедри

_____ Леонід УРИВСЬКИЙ

«___» _____ 20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

**на тему: «Архітектура та технічні принципи функціонування ядра
мережі мобільного зв'язку LTE»**

Виконав:

студент IV курсу, групи ТС-61

Іван ВЕТОШКО _____

Керівник:

Доцент кафедри ТС, доцент,

В'ячеслав НОСКОВ _____

Рецензент:

Незалежний експерт з телекомунікацій, кандидат технічних наук,

Володимир ВАХРУШЕВ _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.

Студент _____

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Програма професійного спрямування (спеціалізація) – «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Леонід УРИВСЬКИЙ

«___» _____ 20__ р.

ЗАВДАННЯ
на дипломну роботу студенту
Ветошку Івану Петровичу

1. Тема роботи **«Архітектура та технічні принципи функціонування ядра мережі мобільного зв'язку LTE»**, керівник роботи Носков В'ячеслав Іванович, доцент, затверджені наказом по університету від **30 березня 2020 р. № 924-с.**

2. Термін подання студентом роботи **12 червня 2020 року.**

3. Вихідні дані до роботи: Інформаційні матеріали щодо систем мобільного зв'язку LTE. Структурований план порядку розробки матеріалів дипломної роботи.

4. Зміст роботи

Обґрунтувати актуальність теми. Розглянути та проаналізувати концептуальні підходи щодо побудови мережі мобільного зв'язку LTE. Розглянути структуру мережі LTE та визначити призначення та функції її ядра (EPC). Детально розглянути принципи побудови ядра мережі LTE з визначенням інтерфейсів взаємодії як в середині ядра, так із іншими структурними елементами мережі. Показати які процеси відбуваються у ядрі при підключенні абонентів за різними сценаріями. Проаналізувати принципи побудови IP мультимедійної підсистеми (IMS), яка розширює

функціональність ЕРС до можливостей обробки телефонних викликів (технологія VoLTE). Деталізувати технологію VoLTE. Виконати аналіз процедур, що відбуваються у ядрі при реєстрації мобільних терміналів у мережі LTE, та навести як забезпечується безпека при передачі інформаційних повідомлень. Провести аналіз основного функціоналу системи управління мережею LTE.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): 1) Тема та цілі дипломної роботи; 2) Структура мережі LTE; 3) Еталонна архітектура ядра мережі LTE; 4) Принцип функціонування мережі LTE при передачі даних; 5) Використання підсистеми IMS в мережі LTE; 6) Висновки по роботі

6. Дата видачі завдання: **13 квітня 2020 року**

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Концептуальні підходи до побудови мережі LTE. Структура мережі та загальний принцип функціонування. Функції елементів ядра мережі (ЕРС).	18.04.2020	
2	Принципи побудови ядра мережі: еталонна архітектура ядра мережі та інтерфейси взаємодії між вузлами ЕРС та іншими підсистемами.	28.04.2020	
3	Система IMS, основні протоколи, процедури та принцип надання голосових послуг. Організація управління «дзвінками» в мережі LTE. Управління доступом в мережу. Забезпечення безпеки в мережі. LTE.	20.05.2020	
4	Система управління мережею LTE: загальний принцип побудови; управління мобільністю; забезпечення ОАМ-функціональності.	26.05.2020	
5	Вступ, Висновки	02.06.2020	
6	Чистовий варіант дипломної роботи, плакати	10.06.2020	

Студент

Іван ВЕТОШКО

Керівник роботи

В'ячеслав НОСКОВ

РЕФЕРАТ

Текстова частина дипломної роботи: 74 с., 22 рис., 1 табл., 38 джерел з переліком посилань.

Мета роботи – дослідження архітектури та технічних принципів функціонування ядра мережі мобільного зв'язку LTE. Виконання аналізу побудови та реалізації IP-мультимедійної підсистеми IMS для організації надання голосових послуг в мережі LTE.

В даній роботі розглядається структура мережі LTE та загальний принцип функціонування, еталонна архітектура ядра мережі та інтерфейси взаємодії з іншими підсистемами, система IMS для забезпечення міграції голосового трафіку з мереж попереднього покоління, основні протоколи взаємодії між вузлами, процедури в мережі LTE та принцип надання голосових послуг, управління доступом та забезпечення безпеки в мережі даного типу, управління мобільністю абонентів та організація систем управління мережею на базі OAM-функціоналу.

МЕРЕЖА LTE, МОДЕРНІЗОВАНЕ ЯДРО EPS, БЛОК УПРАВЛІННЯ МОБІЛЬНІСТЮ MME, ПІДСИСТЕМА IMS, ІНТЕРФЕЙСИ ВЗАЄМОДІЇ, ПРОТОКОЛ SIP, ІДЕНТИФІКАТОР GUTI, ОРГАНІАЦІЯ УПРАВЛІННЯ ВИКЛИКАМИ, ФУНКЦІОНАЛЬНИЙ РІВЕНЬ МЕРЕЖІ.

ABSTRACT

The purpose of the work is study architecture and technical principles of LTE mobile communication network core functioning. Perform analysis of construction and implementation of IP-multimedia subsystem for organization voice services provisioning in the LTE network.

In this paper was discussed the structure of the LTE network and the operation general principles, reference architecture of the network core and interfaces for interaction with other subsystems, IMS system for voice traffic migration from previous generation networks, basic protocols of interaction between nodes, procedures in the LTE network and principle of providing voice services, access control and security in the network of this type, subscriber mobility management and organization of network management systems based on OAM functionality.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ.....	8
ВСТУП	12
1 АРХІТЕКТУРА МЕРЕЖІ LTE.....	13
1.1 Концептуальні підходи до побудови мережі LTE.....	13
1.2 Структура мережі LTE та загальний принцип функціонування.....	14
1.3 Призначення та основні функції мережевих елементів (вузлів) ядра мережі LTE	17
1.4 Висновки з розділу 1	23
2 ПРИНЦИПИ ПОБУДОВИ ЯДРА МЕРЕЖІ LTE.....	24
2.1 Еталонна архітектура ядра мережі та інтерфейси взаємодії між вузлами ЕРС та іншими підсистемами	24
2.2 Система IMS, основні протоколи, процедури та принцип надання голосових послуг.....	35
2.3 Організація управління «дзвінками» в мережі LTE.....	48
2.4 Управління доступом в мережу.....	51
2.5 Забезпечення безпеки в мережі	56
2.6 Висновки з розділу 2.....	60
3 СИСТЕМА УПРАВЛІННЯ МЕРЕЖЕЮ LTE	62
3.1 Управління мобільністю в мережі LTE	62
3.2 ОАМ-функціональність в мережі LTE	65
3.3 Висновки з розділу 3.....	68

					<i>КПІ.924-с.02.ТС-61.2020.ПЗ</i>			
Змн.	Лист	№ докум.	Підпис	Дата				
Розроб.		Ветошко І.П.			Архітектура та технічні принципи функціонування ядра мережі мобільного зв'язку LTE	Літ.	Арк.	Акрушів
Перевір.		Носков В.І.					6	74
Реценз.		Вахрушев В.П.				ІТС		
Н. Контр.		Новіков В.І.						
Затверд.		Уривський Л.О.			Пояснювальна записка			

ВИСНОВКИ.....	69
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:.....	71

					КПІ.924-с.02.ТС-61.2020.ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК СКОРОЧЕНЬ

3GPP	3rd Generation Partnership Project – партнерська організація, котра розробляє специфікації для мобільної телефонії
AAA	Authentication, Authorization, Accounting – функціональний блок автентифікації, авторизації та обліку
A-BG	Access Border Gateway – шлюз доступу
AF	Application Function – прикладні функції
AIPN	All-IP Network – мережа, котра заснована на роботі протоколу IP
AS	Authentication Server – сервер автентифікації
BGCF	Breakout Gateway Control Function – функція управління шлюзами переривання
CDR	Call Detail Records – детальні записи викликів
CP	Control Plane – площина управління
CSCF	Call Session Control Function – функція управління сеансом зв'язку
E-CSCF	Emergency CSCF – CSCF для екстрених служб
eNB	Evolved NodeB (eNodeB) – модернізована базова станція
ENUM	E.164 Number Mapping – спеціальна база даних для номерів телефонного формату
EPC	Evolved Packet Core – модернізоване пакетне ядро
ePDG	evolved P-GW – модернізований шлюз пакетної мережі
EPS	Evolved Packet System – модернізована пакетна система
E-UTRAN	Evolved Universal Terrestrial Radio Access Network – модернізована підсистема мережі радіодоступу
GBR	Guaranteed Bit Rate – гарантована бітова швидкість
GGSN	Gateway GPRS Support Node – шлюзовий вузол в мережах попереднього покоління
GPRS	General Packet Radio Service – сервіс пакетної радіопередачі

GSM	Global System for Mobile Communications – глобальний стандарт цифрового мобільного зв'язку
GTP	GTP – протокол тунелювання GPRS
GTP-C	GTP Control Plane – протокол GTP в площині управління
GTP-U	GTP User Plane – протокол GTP в користувацькій площині
GUTI	Globally Unique Temporary Identity – глобальний унікальний тимчасовий ідентифікатор
HSS	Home Subscriber Server – домашній сервер абонентів
IBCF	Interconnect Border Control Function – функція контролю з'єднань між різними мережами
I-CSCF	Interrogating CSCF – запитуючий CSCF
IETF	Internet Engineering Task Force - відкрите міжнародне співтовариство проектувальників
IFC	Initial Filter Criteria – початкові критерії фільтрації
IMS	IP Multimedia Subsystem – IP-мультимедійна підсистема
IMSI	International Mobile Subscriber Identity – постійний ідентифікатор абонента
IPsec	IPsecurity – протокол безпеки
ISDN	Integrated Services Digital Network – цифрова мережа з інтегрованими службами
ISUP	ISDN User Part – протокол спільноканальної сигналізації №7
LTE	Long Term Evolution – довготривалий розвиток
MGCF	Media Gateways Control Function – функція управління медіашлюзами
MGW	Media Gateway – медіашлюз
MME	Mobility Management Entity – блок управління мобільністю
NAS	Non-Access Stratum – функціональний рівень без доступу
OAM	Operation, Administration and Management – операції, адміністрування та управління в мережі

OSS	Operation Support Subsystem – підсистема підтримки операцій
PCEF	Policy and Charging Enforcement Function – функціональний компонент в шлюзі P-GW
PCRF	Policy and Charging Resource Function – функціональний компонент, що управляє політиками та тарифікацією у реальному часі
P-CSCF	Proxy CSCF – проксі CSCF
PDN	Packet Data Network – мережа пакетних даних
P-GW	PDN Gateway – шлюз пакетної мережі
PLMN	Public Land Mobile Network – мережа мобільного оператора
PSTN	Public Switched Telephone Network – телефонна мережа загального користування
QCI	QoS Class Identifier – ідентифікатор класу QoS
QoS	Quality of Service – якість обслуговування
RFC	Request For Comment – запит на коментарі
RNC	Radio Network Controller – контролер радіомережі в UMTS
RRC	Radio Resource Control – протокол управління радіоресурсами
RTP	Real-Time Transport Protocol – протокол транспортування медіапотоків у реальному часі
S-CSCF	Serving CSCF – обслуговуючий CSCF
SCTP	Stream Control Transmission Protocol – це протокол передачі управління потоком
SDP	Session Description Protocol – протокол опису сеансів
S-GW	Serving Gateway – обслуговуючий шлюз
SIP	Session Initiation Protocol – протокол ініціації сеансу
SRVCC	Single Radio Voice Call Continuity – процедура безперервного голосового виклику
TA	Tracking Area – область відслідковування
TAI	Tracking Area Identity – ідентифікатор області

відслідковування

TAS	Telephony Application Server – сервер телефонних додатків
TAU	Tracking Area Update – оновлення області відслідковування
TLS	(Transport Layer Security)
TMN	Telecommunication Management Network – управління мережами зв’язку
TMSI	Temporary Mobile Subscriber Identity – тимчасовий ідентифікатор абонента
TS	Technical Specification – технічна специфікація
UDP	User Datagram Protocol – протокол користувацьких датаграм
UE	User Equipment – користувацьке обладнання
UMTS	Universal Mobile Telecommunications System – універсальна мобільна телекомунікаційна система
UP	User Plane – користувацька площина
USIM	Universal Subscriber Identity Module – універсальний модуль ідентифікації абонента
VoLTE	Voice over LTE – технологія передачі голосу в мережі LTE
Wi-Fi	Wireless Fidelity – технологія бездротової локальної мережі
WiMAX	Worldwide Interoperability for Microwave Access – надання універсального бездротового зв’язку на великих відстанях для широкого спектру пристроїв

ВСТУП

Сьогодення вимагає від мережі мобільного зв'язку LTE високої доступності, надійності та впровадження нових технологій таких, як передачу голосового трафіку у вигляді IP-пакетів. Модернізоване пакетне ядро є опорним елементом мережі для управління всіх процесів мобільних терміналів та взаємодії з іншими підсистемами. Детальний аналіз архітектури ядра мережі LTE дозволяє з'ясувати можливість введення нових сервісів та покращення якості обслуговування абонентів.

Мережі LTE широко впроваджуються у різних країнах світу. Завдяки ефективному використанню ресурсів, високому рівню безпеки та чіткому розподілу функцій між мережевими елементами, подальший розвиток ядра EPS є перспективним, оскільки, основні принципи побудови та технічного функціонування опорного ядра EPS є еталоном для мобільної мережі наступного покоління 5G. Організація та застосування підсистеми IMS, що працює, як доповнення до модернізованого ядра, дозволяє здійснити міграцію голосового трафіку з мереж із комутацією каналів в LTE. Під час розробки нового стандарту мобільного зв'язку, потреба у вивченні та вдосконаленні опорного ядра EPS тільки зростає. Тому тема даної роботи є актуальною.

Метою даної кваліфікаційної роботи являється проведення аналізу архітектури та технічних принципів функціонування ядра мережі мобільного зв'язку LTE, а також дослідження способів модернізації та вдосконалення даної мережі за рахунок впровадження нових технологій.

1 АРХІТЕКТУРА МЕРЕЖІ LTE

1.1 Концептуальні підходи до побудови мережі LTE

Сьогодні, коли обсяги споживання мобільного трафіку щодня збільшуються, перед інженерами електрозв'язку постало чітке завдання – забезпечити потреби користувачів. Тому впровадження мереж четвертого покоління, покликане на покращення основних показників пакетної передачі даних.

Архітектура мережі LTE розроблена таким чином, щоб забезпечити підтримку пакетного трафіку з так званою «безшовною» мобільністю, високими показниками якості обслуговування та мінімальними затримками доставки пакетів.

Система LTE призначена для того, щоб надати користувачам доступ до нових сервісів та до мережі інтернет за допомогою протоколу IP. Основна відмінність від мереж попереднього покоління – це відсутність голосового домену. Таким чином, LTE працює виключно з комутацією пакетів, тоді як в мережах другого та третього покоління спостерігається розділення на каналну комутацію, для передачі голосу і пакетну комутацію, для передачі даних.

В мережі LTE присутня велика кількість різних вузлів, кожен з яких виконує певні завдання. Всі вузли прийнято поділяти на дві підсистеми: мережа радіодоступу (Evolved Universal Terrestrial Radio Access Network, E-UTRAN) та модернізоване пакетне ядро (Evolved Packet Core, EPC). Вузол eNB (Evolved NodeB) поєднує в собі функції базової станції та контролера радіомережі. Користувацький трафік проходить через нього й далі по інтерфейсу S1 потрапляє до ядра мережі, де відбувається подальша обробка даних. Структуру мережі LTE прийнято називати «пласкою», оскільки майже всі мережеві взаємодії відбуваються між двома вузлами: базовою станцією eNodeB та блоком управління мобільністю MME (Mobility Management Entity) [1].

Важливим фактором, для впровадження нової технології LTE, є можливість забезпечення мобільності. Дана функція мережі поділяється на два види: дискретна мобільність (роумінг) та неперервна мобільність (хендовер). Для того, щоб забезпечити процедури неперервного з'єднання LTE-абонентів (терміналів), потрібно максимально (повсюдно) розширювати покриття послуг безпроводового широкосмугового доступу.

В основу принципів побудови LTE, подібно до мереж третього покоління, покладено поділ двох аспектів, а саме: фізичної реалізації окремих мережевих блоків та формування функціональних зв'язків між ними. Задача фізичної реалізації вирішується, виходячи з концепції області (domain), а функціональні зв'язки розглядаються в рамках площини (stratum). Основною перевагою LTE перед мережею попереднього покоління є зниження затримки при передачі користувацьких даних та управляючої інформації. Це обумовлено тим, що вони проходять через менше число проміжних елементів.

Вагомим кроком до початку технічного проектування мереж LTE, був вихід Release 8 [2], виданий партнерською асоціацією груп телекомунікаційних компаній (3rd Generation Partnership Project, 3GPP). Розробники відмовились від технології широкосмугового множинного доступу із кодовим розподілом каналів (Wideband Code Division Multiple Access, W-CDMA) та перейшли до більш новітньої і прогресуючої технології множинного доступу з ортогональним частотним розподілом (Orthogonal Frequency-Division Multiple Access, OFDMA). Робота ядра мережі EPC заснована на технології IP. Тому таку структуру прийнято відносити до мереж AIPN (All-IP Network) [3].

1.2 Структура мережі LTE та загальний принцип функціонування

Мережа LTE складається з двох найважливіших компонентів: мережі радіодоступу E-UTRAN та опорної мережі EPC.

На рис. 1.1 зображена структура мережі LTE.

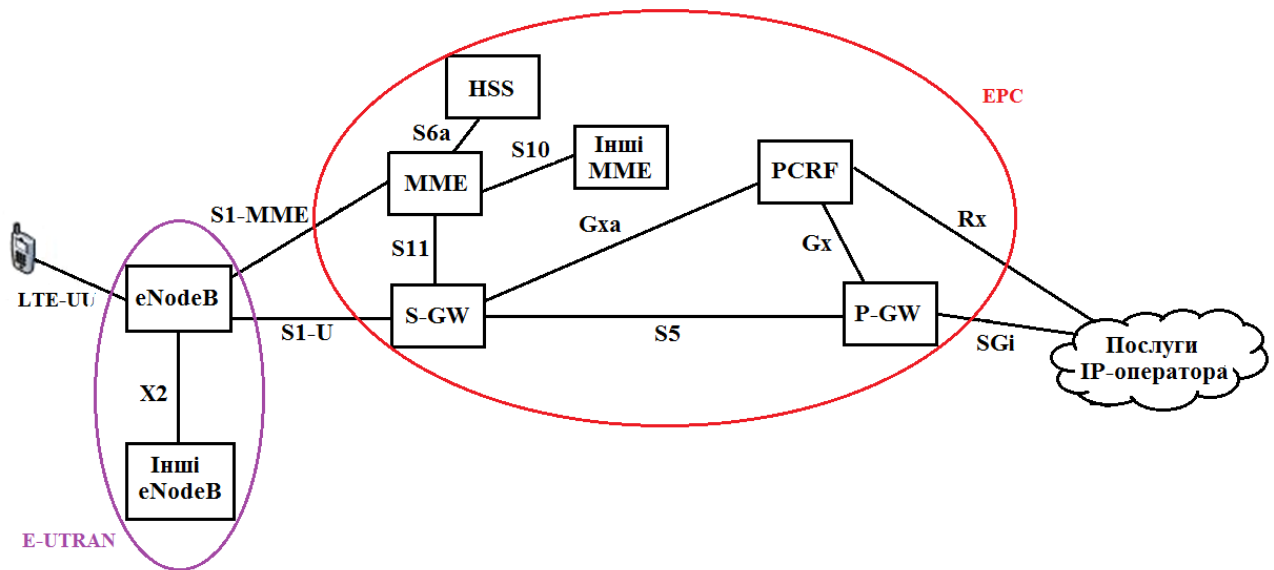


Рисунок 1.1 Структура мережі LTE

Мережа радіодоступу в LTE збудована, як сукупність нових базових станцій eNodeB. Завдяки ним, зникає потреба вводити в структурі окремий контролер радіомережі. Оскільки вони акумулюють в собі всі функції і завдання базової станції NodeB та контролера RNC мереж третього покоління. Вузли eNB з'єднані між собою інтерфейсом X2, а також за допомогою інтерфейсу S1 вони підключені до ядра мережі EPC. Взаємодія з блоком управління мобільності відбувається по S1-MME, а з обслуговуючим шлюзом (Serving Gateway, S-GW) по S1-U.

Підсистему радіодоступу мереж четвертого покоління називають E-UTRAN. Це модернізована підсистема мереж третього покоління. Вона складається лише з одного вузла eNB, котрий взаємодіє з користувацьким обладнанням (User Equipment, UE) по радіоінтерфейсу LTE-UU. Завдяки спрощеній моделі, можливе зниження затримки всіх операцій радіоінтерфейсу. В E-UTRAN дотриманий принцип логічного розділення транспортних мереж передачі даних та сигналізації.

На рис. 1.2 зображена базова архітектура підсистеми радіомережі E-UTRAN.

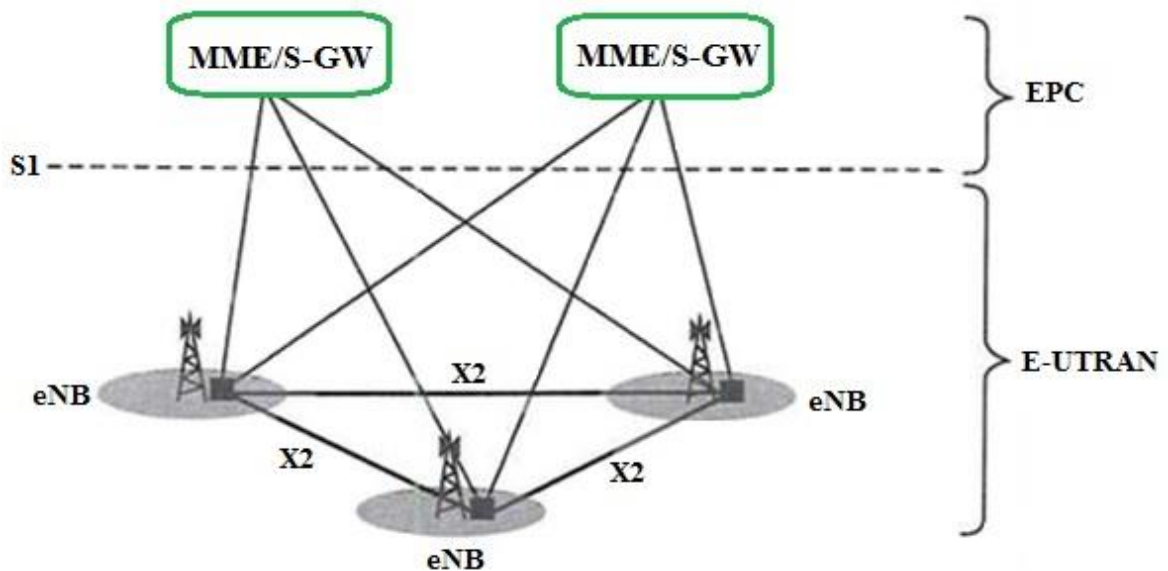


Рисунок 1.2 Базова архітектура підсистеми радіомережі E-UTRAN

Основні функції базової станції eNodeB:

- забезпечення передачі трафіку та сигналізації по радіоканалу;
- управління радіоресурсами: розподіл радіоканалів, динамічний розподіл ресурсів (scheduling);
- підтримка синхронізації передач та контроль рівня завад в соті;
- вибір MME та організація сигнального обміну з ним;
- забезпечення шифрування та цілісності передачі по радіоканалу;
- виконання стиснення заголовків IP-пакетів.

Для організації хендверів між сусідніми базовими станціями та балансування навантаження між ними використовують інтерфейси X2. Важливою характеристикою даних інтерфейсів є те, що вони можуть бути логічними, тобто для їх організації не обов'язково реальне фізичне з'єднання між сусідніми eNB.

По інтерфейсу S1-MME передається сигнальна інформація між eNB та блоком управління мобільності. S1-U відповідає за передачу даних між eNB та обслуговуючим шлюзом. eNB може мати з'єднання з декількома S-GW.

До користувацького обладнання відносять сукупність терміналів з різними рівнями функціональних можливостей, що використовуються

мережевими абонентами для доступу до LTE-послуг. В якості користувачького терміналу може бути не тільки «живий» абонент, що, до прикладу, користується послугами голосового трафіку, а й пристрій для передачі та прийому певних мережових або призначених для користувачів додатків.

ММЕ працює тільки зі службовою інформацією, тому IP-пакети, які містять користувачьку інформацію, через нього не проходять. Це надає певні переваги. Оскільки у такому випадку, пропускну здатність мережі можна нарощувати незалежно, як для трафіку користувачів, так і для службової інформації. В ядрі мережі можна виділити два основні шлюзи, а саме: обслуговуючий шлюз S-GW та шлюз пакетної мережі (Packet Data Network Gateway, P-GW). S-GW функціонує, як блок управління локальною мобільністю. Він приймає та перенаправляє пакети даних, що відносяться до базової станції та обслуговуючих ним терміналів користувачів. В свою чергу P-GW виступає інтерфейсом між набором eNB та різними зовнішніми мережами [4].

1.3 Призначення та основні функції мережових елементів (вузлів) ядра мережі LTE

Evolved Packet Core являється опорною мережею LTE. Вона сильно відрізняється від базової мережі GSM/GPRS (Global System for Mobile Communications/General Packet Radio Service), що використовується в мережах другого покоління та WCDMA/HSPA (Wideband Code Division Multiple Access/High Speed Packet Access), що є технологіями в мережах третього покоління. Модернізоване ядро EPC підтримує тільки пакетну комутацію і зазвичай відповідає за управління UE та встановлення каналів передачі. В модернізованій пакетній системі (Evolved Packet System, EPS), що складає мережу LTE, канали передачі використовуються для трансляції IP-трафіку від шлюза PDN до UE. Канал зв'язку може розглядатись як IP-канал

з визначеною якістю обслуговування QoS (Quality of Service) між шлюзом та терміналом. EPS має «плоску» IP-архітектуру, котра дозволяє мережі ефективно і без зайвих навантажень обробляти великий обсяг трафіку даних.

На рис. 1.3 зображена більш детально архітектура модернізованого ядра EPS.

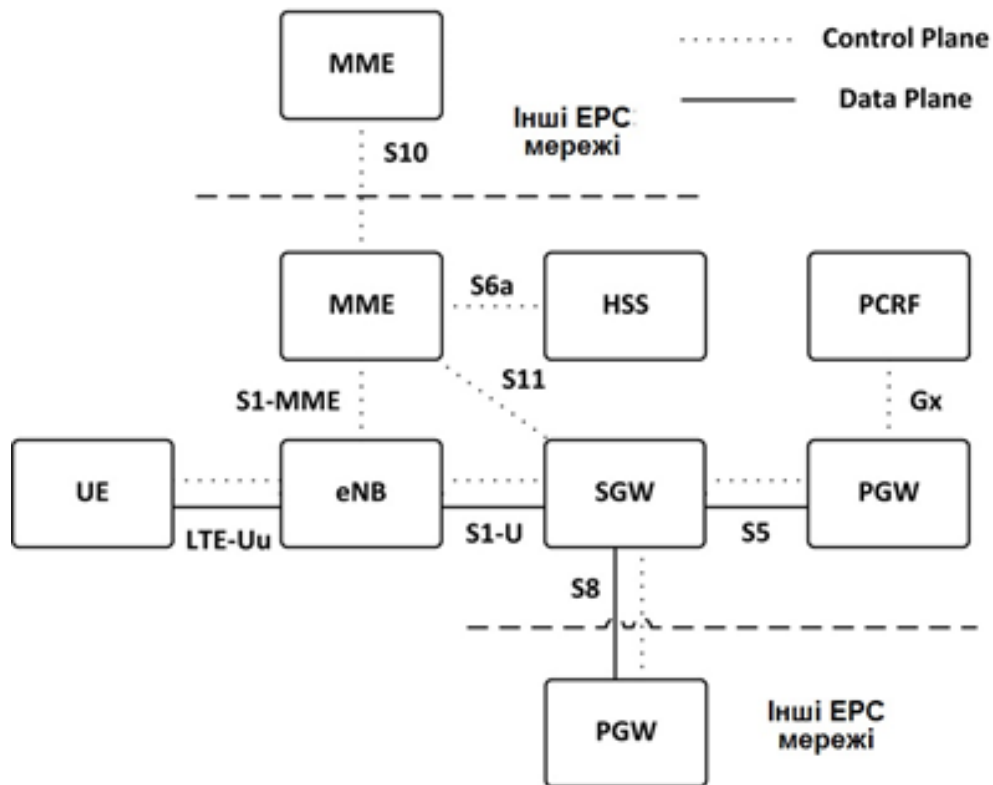


Рисунок 1.3 Архітектура EPS

Пунктирною лінією зображено площину управління (Control Plane, CP), для сигнальних з'єднань. Суцільною лінією зображено з'єднання для передачі даних (Data Plane, DP). Таким чином відбувається розділення сигнальної та користувацької інформації по окремим виділеним каналам.

Блок управління мобільністю (MME) грає важливу роль в архітектурі LTE EPS. Фактично MME являється основним вузлом сигналізації в ядрі мережі. Він відповідає за ініціювання пейджингу та автентифікацію мобільного пристрою. MME зберігає інформацію про місцезнаходження на рівні області відслідковування (Tracking Area, TA) для кожного користувача, а також обирає відповідний шлюз в процесі його реєстрації. У випадку, коли

навантаження сигналізації в мережі зростає, можуть використовувати декілька вузлів MME. Тоді їх згруповують разом і вони працюють, як один логічний розподілений вузол. Блок управління мобільністю з'єднаний з HSS (Home Subscriber Server) домашньої мережі по інтерфейсу S6a. Інтерфейс S10 дозволяє з'єднувати між собою MME різних мереж. Це дозволяє обслуговувати UE при переміщеннях абонента, а також при його знаходженні в роумінгу. У випадку, коли інтерфейс X2 недоступний, MME передає повідомлення хендовера між eNB.

MME виконує наступні функції:

- передає захищену інформацію про точки доступу до послуг та забезпечує захищене управління точками доступу;
- управляє списком областей відслідковування;
- передає інформацію в базову мережу для управління мобільністю між різними мережами радіодоступу;
- управляє базовими станціями eNodeB, що знаходяться в стані очікування (Idle Mode), а також виконує перенаправлення викликів;
- обирає обслуговуючий та пакетний шлюз для мереж радіодоступу різних стандартів;
- забезпечує послуги роумінгу;
- обирає новий блок управління мобільністю при виконанні хендоверу;
- виконує автентифікацію терміналів;
- підтримує передачу повідомлень PWS (Public Warning System);
- управляє радіоканалом та виконує встановлення виділеного каналу.

Обслуговуючий шлюз S-GW являється якірною структурою, що забезпечує мобільність абонентів. Він з'єднує ядро мережі та підсистему радіодоступу. Кожен працюючий UE обслуговує відповідний S-GW. Всі IP-пакети мобільних терміналів маршрутизуються через нього. У випадку, коли UE вільний і не зайнятий, обслуговуючий шлюз вимикає низхідний канал даних (Down Link, DL) та виконує пейджинг. Він управляє та зберігає

стан мобільного терміналу.

S-GW виконує наступні функції:

- відповідає за вибір точки прив'язки («якоря») локального місцезнаходження (Local Mobility Anchor) при хендовері;
- виконує буферизацію пакетів даних в низхідному напрямку, призначених для мобільних терміналів, що знаходяться в режимі очікування та ініціація процедури запиту послуг;
- виконує маркування пакетів транспортного рівня;
- виконує маршрутизацію та перенаправлення пакетів даних;
- забезпечує санкціоноване перехоплення користувацької інформації;
- виконує тарифікацію абонентів;
- забезпечує формування облікових записів користувачів та ідентифікатора класу якості обслуговування для тарифікації.

Шлюз пакетної мережі P-GW організовує точку доступу до зовнішніх IP-мереж. Відповідно, він є якірним шлюзом для забезпечення трафіку. P-GW відповідає за розподіл IP-адрес для всіх UE. Якщо абонент має статичну IP-адресу, то P-GW її активує. У випадку, коли абонент на час сеансу зв'язку має отримати динамічну IP-адресу, P-GW запрошує її у сервера DHCP (Dynamic Host Configuration Protocol) або сам виконує необхідні функції DHCP, після чого забезпечує доставку IP-адреси абоненту. P-GW виконує реалізацію QoS з гарантованою бітовою швидкістю (Guaranteed Bit Rate, GBR). В склад P-GW входить функціональний елемент PCEF (Policy and Charging Enforcement Function), котрий забезпечує якісні характеристики послуг на зовнішньому з'єднанні через інтерфейс SGi та фільтрацію пакетів даних. UE може бути підключеним до більш ніж одного P-GW при зверненні до декількох PDN (Packet Data Network). Якщо абонент знаходиться в домашній мережі, функції обслуговуючого та пакетного шлюзу можуть виконувати як два різних вузли, так і один. Тоді між вузлами S-GW та P-GW встановлюється тунельне з'єднання по інтерфейсу S5. Коли мобільний термінал здійснює доступ у візитну PDN (наприклад, при обслуговуванні в

роумінгу), тоді вузли S-GW та P-GW знаходяться в різних мережах. У такому випадку взаємодія між даними вузлами відбувається за допомогою інтерфейсу S8.

P-GW виконує наступні функції:

- фільтрує користувацькі пакети;
- виконує санкціоноване перехоплення користувацької інформації;
- забезпечує тарифікацію послуг та їх селекцію за рахунок підрахунку використаного обсягу даних;
- виконує маркування пакетів транспортного рівня в низхідному напрямку;
- забезпечує розподіл IP-адрес для мобільних терміналів.

Домашній сервер абонентів (Home Subscriber Server, HSS) являється ключовим елементом структури мобільної мережі LTE. HSS – це централізована база даних, що містить інформацію про абонентів (їхні профайли). Вона дозволяє провайдерам послуг зв'язку управляти абонентами в режимі реального часу. Також HSS дозволяє виконувати спеціалізовані функції, такі як: заборона окремих послуг, активація та деактивація SIM-карт, створення ієрархічного розподілу абонентів на основі їх підписок. Роль HSS заключається у взаємодії з мережею, наданні профайлу абонента та інформації автентифікації. Дані про абонентів, що містяться в базі даних допомагають при авторизації. На базі HSS побудований сервер автентифікації (Authentication Server, AS). У мережах попереднього покоління він був окремим вузлом і мав назву центра автентифікації (Authentication Center, AuC). Таким чином, сервер автентифікації відповідає за генерацію інформації безпеки з ключів ідентифікації користувача, а також забезпечує функціонування блоку AAA (Authentication, Authorization, Accounting). Мережа LTE може включати один або декілька HSS. Їхня кількість залежить від географічної структури мережі та числа абонентів. Проте, при наявності двох чи більше домашніх серверів абонентів, вони повинні взаємодіяти один з одним та оновлювати свої бази даних, оскільки

серверам необхідно мати синхронізовану базу даних для коректної роботи.

HSS виконує наступні функції:

- підтримка автентифікації та реєстрації абонентів, завантаження профілів абонентів до MME;
- підтримка автентифікації та реєстрації абонентів в мережах не-3GPP (наприклад, Wi-Fi), передача профілів абонентів в AAA;
- забезпечення роумінгових обмежень;
- забезпечення обмеження сервісів;
- забезпечення обмеження по типам мереж доступу;
- взаємодія з іншими елементами мережі по протоколам на основі DIAMETER.

Функціональний компонент, що управляє політиками та тарифікацією у реальному часі, має назву PCRF (Policy and Charging Resource Function). Він представляє собою управляючий сервер, що забезпечує централізоване управління ресурсами мережі, облік і тарифікацію послуг, що надаються абоненту. Коли з'являється запит на нове активне з'єднання, ця інформація надходить на PCRF. Тоді він оцінює наявні в нього ресурси мережі та направляє в PCEF шлюзу P-GW команди, які встановлюють вимоги до якості послуг та їх тарифікації. PCRF надає правила для різних абонентських груп по виділенню каналів зі специфічними параметрами якості сервісу та відповідно до них встановлює правила тарифікації. Сервер PCRF являє гнучку та масштабовану програмну платформу для розробки і управління політиками різного типу, що спеціалізовані в телекомунікаційній сфері. Також він взаємодіє з P-GW по інтерфейсу Gx, побудованому на основі протоколу DIAMETER.

PCRF виконує наступні функції:

- надає можливість управління мережею та абонентською політикою в режимі реального часу;
- забезпечує ефективну та динамічну маршрутизацію потоків, а також визначає пріоритети мережевого трафіку;

- надає єдине представлення контексту абонента на основі комбінації даних про пристрій, мережі, місцезнаходження та білінгу;
- встановлює відповідні правила тарифікації;
- збирає та аналізує білінгові дані з інших вузлів EPC [5].

1.4 Висновки з розділу 1

У даному розділі розглянуто концептуальні підходи до побудови мережі LTE. Проведений аналіз структури мережі та наведений загальний принцип її функціонування. Також здійснено детальний аналіз основних вузлів ядра EPC в мережі LTE.

Структура LTE складається з двох компонентів: мережі радіодоступу E-UTRAN та опорної мережі EPC. Оскільки опорна мережа заснована на роботі технології IP, то таку структуру прийнято відносити до мереж All-IP (All-IP Network). Підсистема E-UTRAN побудована, як сукупність нових базових станцій eNodeB, що включають в себе функції контролера радіомережі. Головним вузлом модернізованого пакетного ядра є блок управління мобільністю MME, котрий працює тільки зі службовою інформацією та відповідає за ініціювання пейджингу та автентифікацію мобільного пристрою. Наявність «плоскої» IP-архітектури в мережі даного типу дозволяє ефективно і без зайвих навантажень обробляти великий обсяг трафіку даних. Основною перевагою LTE перед мережею попереднього покоління є зниження затримки при передачі користувацьких даних та управляючої інформації.

2 ПРИНЦИПИ ПОБУДОВИ ЯДРА МЕРЕЖІ LTE

2.1 Еталонна архітектура ядра мережі та інтерфейси взаємодії між вузлами EPC та іншими підсистемами

Еталонна архітектура EPC, що описана в технічній специфікації партнерської організації 3GPP TS 23.002 [6], перерозподіляє функції мережевих елементів порівняно з мережами UMTS. Наприклад, функції протоколів площини управління сервісного вузла SGSN стають функціями блока управління мобільністю MME, а функції тимчасової бази даних абонентів VLR (Visitors Location Register) переходять у функціонал HSS. Основними вузлами даної мережі є: MME, HSS, S-GW, P-GW та PCRF. Архітектура EPC забезпечує відсутність дублювання функцій мережевих протоколів та максимально спрощує структуру порівняно з мережами третього покоління. EPC є повністю пакетним доменом для мережі LTE, котра надає всю сукупність IP-послуг на основі технології пакетної комутації даних. Доступ до базової мережі EPC може здійснюватись як через мережі радіодоступу другого та третього покоління, наприклад, UTRAN (UMTS Terrestrial Radio Access Network) і GERAN (GSM EDGE Radio Access Network), так і через мережі радіодоступу нестандартизованих технологій проектом 3GPP (наприклад, мережі IEEE: Wi-Fi та WiMAX). Також доступ може здійснюватись через проводові IP-технології, такі як ADSL+ (Asymmetric Digital Subscriber Line) та FTTH (Fiber to the Home).

Окремо можна виділити вид доступу в пакетну опорну мережу LTE через ненадійні мережі Wi-Fi за допомогою спеціалізованого шлюза ePDG (evolved P-GW). Він взаємодіє з пакетним шлюзом P-GW через інтерфейс S2b, на котрому може використовуватись протокол IPv6 або протокол GTP. Даний вид доступу дозволяє впроваджувати нові сервіси. Таким чином, використовуючи в якості останньої милі звичайний Wi-Fi, можна організувати передачу голосових дзвінків (Voice over Wi-Fi) в мережі LTE. UE підключається через інтерфейс SWm до ePDG з використанням

протоколу IPsec, потім відбувається автентифікація і збірка доступних послуг через вузол HSS.

ePDG – це модернізований шлюз пакетних даних, котрий призначений для забезпечення «прозорі» інтеграції Wi-Fi, як підмножини радіодоступу LTE з цільовою апаратною платформою. Наявність даного шлюзу дає можливість безпечно і економічно інтегрувати ненадійні мережі Wi-Fi в ядро мережі. ePDG є високомасштабованим і комплексним рішенням для забезпечення безпеки між ненадійними мережами Wi-Fi та LTE [7].

Еталонна архітектура ядра мережі EPC із вказаними інтерфейсами взаємодії між вузлами зображена на рис. 2.1.

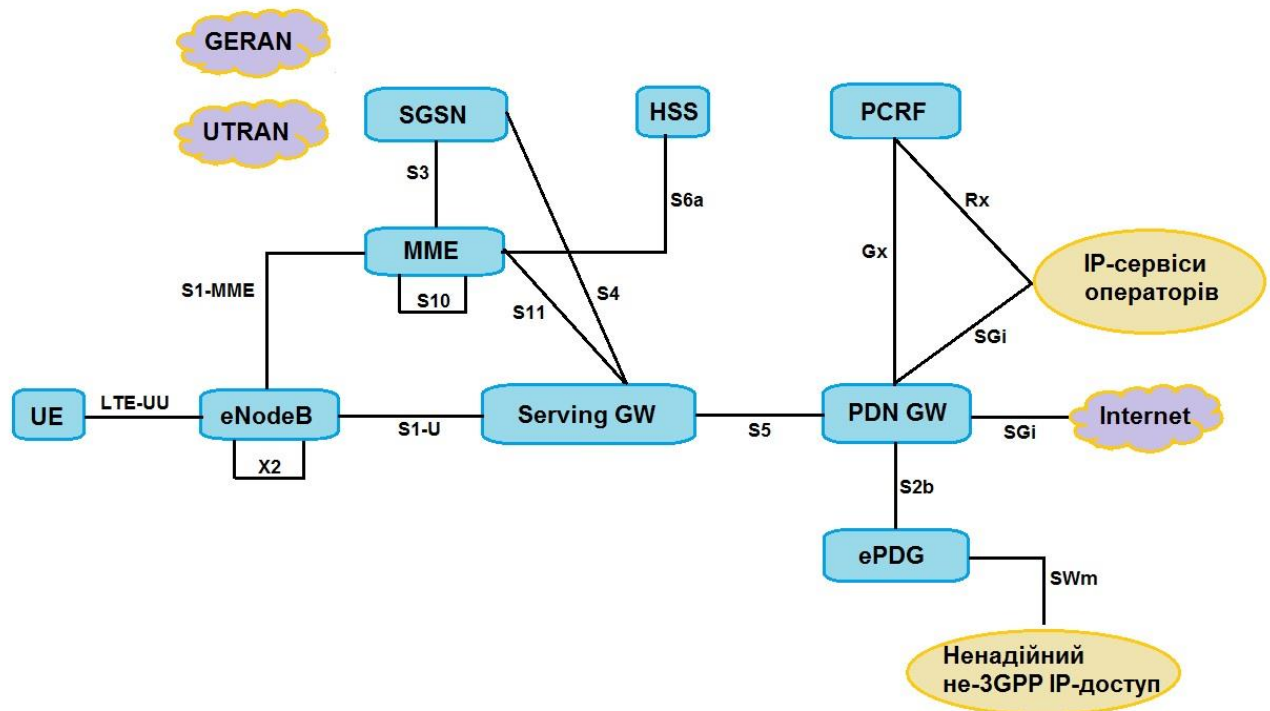


Рисунок 2.1 Еталонна архітектура ядра мережі LTE

Основними функціями модернізованого ядра мережі EPC є:

- управління доступом до мережі;
- процедура автентифікації;
- маршрутизація та передача пакетів;
- управління мобільністю;

- забезпечення безпеки;
- управління радіоресурсами;
- управління мережею;
- забезпечення тарифікації.

Функція вибору мережі або мережі доступу дає можливість абонентському терміналу обирати мережу мобільного зв'язку або мережі доступу, завдяки котрій буде здійснюватись IP-з'єднання абонентського терміналу з сервісними платформами. Вибір мережі або мережі доступу залежить від використовуваних цими мережами технологій. Для мереж стандартів 3GPP принципи вибору мережі визначені в технічній специфікації TS 23.122 [8] та TS 43.022 [9]. Для мереж стандартів не-3GPP, що теж базуються на IP-протоколі, принципи вибору мережі визначені в технічній специфікації TS 23.402 [10].

Функція автентифікації та авторизації дозволяє перевірити справжність абонента. У відповідності до його профілю, визначається доступність мережевих послуг. Функція автентифікації тісно пов'язана з функцією управління мобільністю абонента.

За допомогою функції маршрутизації визначається маршрут передачі і транспортування пакетів даних. Він може бути прокладений як всередині однієї мережі мобільного зв'язку, так і між декількома мережами. Маршрут транспортування пакетів даних встановлюється на основі таблиць маршрутизації та являє собою перелік мережевих вузлів: вихідний вузол, проміжні вузли і вузол призначення. Оскільки LTE працює на основі IP-протоколу, то використовують стандартні механізми маршрутизації і транспортування даних IP-мереж.

Функція управління мобільністю дає змогу стежити за місцезнаходженням абонентського терміналу в мережі E-UTRAN з високою точністю, а саме до однієї зони відслідковування мобільного терміналу (Tracking Area, TA).

Функція забезпечення безпеки, що описана в технічній специфікації

TS 33.401 [11], виконує ряд основних задач:

- захист від несанкціонованого використання послуг мережі LTE;
- забезпечення конфіденційності автентифікації абонента, завдяки використанню тимчасових ідентифікаторів та ключів шифрування;
- забезпечення конфіденційності абонентських даних за допомогою шифрування;
- ідентифікація абонентського термінала.

Функція управління радіоресурсами пов'язана з розподілом ресурсів мережі E-UTRAN між абонентськими терміналами. Блок управління мобільністю MME забезпечує передачу базовій станції eNodeB параметра RFSP (RAT/Frequency Selection Priority), котрий визначає пріоритет радіотехнології та пріоритет вибору частоти. Параметр RFSP використовується базовою станцією для реалізації стратегії по управлінню радіоресурсами.

Функція управління мережею може включати в себе перерозподіл навантаження між вузлами MME. Це дає можливість передавати активну сесію абонентського термінала від одного MME до іншого в процесі обслуговування.

Передача корисного IP-навантаження відбувається по сигнальним з'єднанням та тунелям. Кожне з'єднання між вузлами мережі відповідає певним інтерфейсам та протоколам по яким вони взаємодіють. Сигналізація по інтерфейсах Gx та Rx використовується для відповідних політик QoS. Сигнальне з'єднання через інтерфейс LTE-Uu утворює радіотунель, котрий відповідає за контроль радіоресурсів (Radio Resource Control, RRC) від мобільного термінала до базової станції eNodeB. P-GW взаємодіє із зовнішнім каналом зв'язку по інтерфейсу SGI. Встановлення тунеля по інтерфейсу S5 за допомогою протоколу GTP, забезпечує проходження сигналізації між шлюзами S-GW та P-GW [12].

На рис. 2.2 зображено стандартне підключення в мережі LTE без роумінгу в інші підсистеми. Темною лінією зображена управляюча площина

(Control Plane), по якій передається сигнальна інформація. Світлою лінією зображена користувацька площина (User Plane), по якій передаються дані користувача (корисне навантаження). Таким чином, під час подібного з'єднання, абонент знаходиться в домашній мережі. Корисне навантаження маршрутизується через інтерфейси LTE-Uu, S1-U, S5 та SGi.

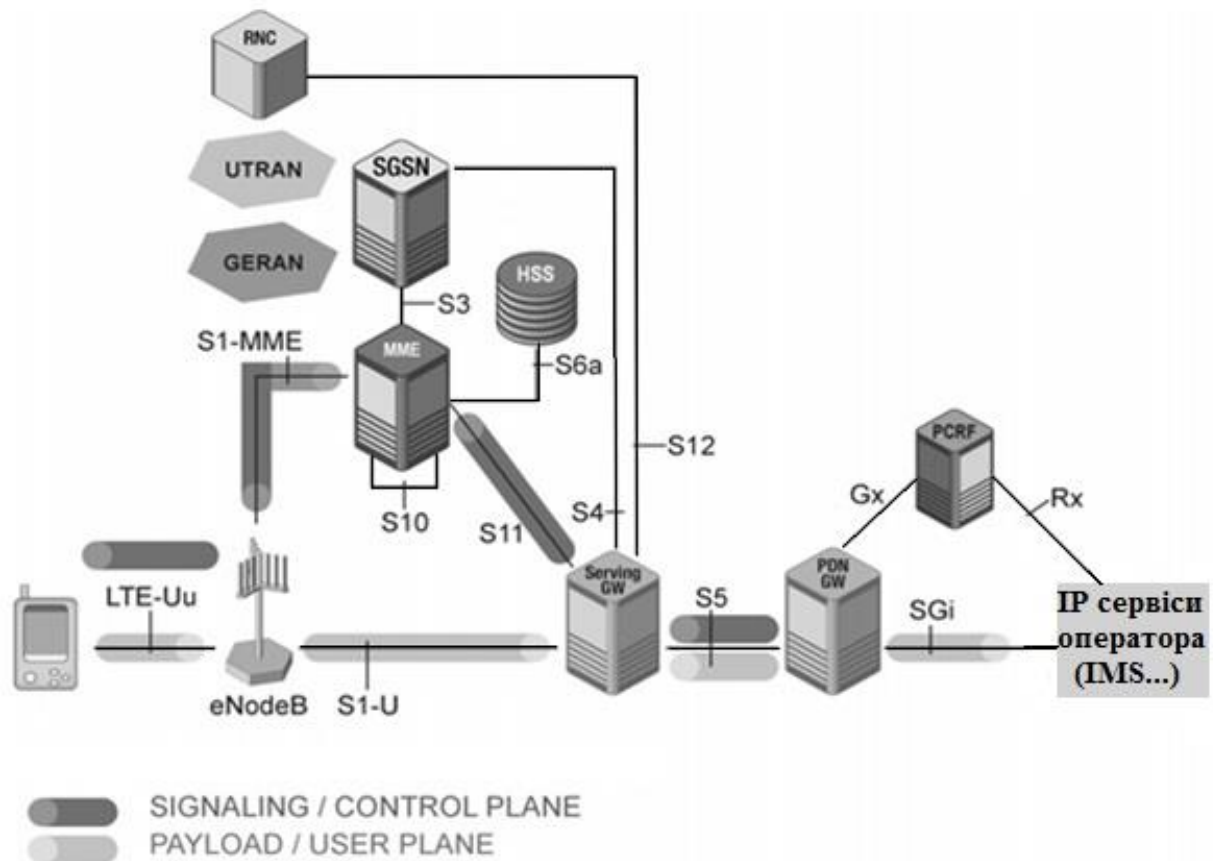


Рисунок 2.2 Підключення в мережі LTE без роумінгу

Розглянемо більш детально призначення та основні функції інтерфейсів, завдяки котрим відбувається взаємодія між різними вузлами мережі LTE та іншими підсистемами.

S1-MME – це інтерфейс управління між базовими станціями E-UTRAN та вузлом управління мобільністю MME. На основі нього працює прикладний протокол S1AP (S1 Application Protocol). По даному інтерфейсу проходить тільки сигнальна інформація.

S1-U – це інтерфейс між базовими станціями E-UTRAN та обслуговуючим шлюзом S-GW, котрий забезпечує передачу даних

користувачів. В ньому використовується протокол GTP-U (GTP User Plane).

S3 – це інтерфейс між вузлом управління мобільністю MME і сервісним шлюзом SGSN (Serving GPRS Support Node). Він забезпечує мобільність користувачів між мережами LTE та UMTS/GPRS. По даному інтерфейсу відбувається обмін сигнальної інформації UE для здійснення хендоверу в мережі попереднього покоління. Якщо з'єднання спершу було встановлено в E-UTRAN, а потім передано в UTRAN/GERAN, то відповідні потоки користувацької площини UP будуть маршрутизуватися по інтерфейсу S4. В протилежному випадку, коли відбувається передача обслуговування з UTRAN/GERAN в мережу E-UTRAN, тунель користувацької площини, по якому передаються дані, може бути «плавно» переключений між інтерфейсами S4 та S1-U під час хендоверу без втрати з'єднання. По інтерфейсу S3 працює протокол GTP-C (GPRS Tunneling Protocol – Control Plane).

S4 – це інтерфейс між обслуговуючим шлюзом S-GW та сервісним шлюзом мереж попереднього покоління SGSN, що забезпечує передачу даних користувачів при хендовері зі зміною мережі доступу, а також передачу даних об'єднаної мережі LTE/UMTS, у котрої відсутній шлюз GGSN (Gateway GPRS Support Node). По інтерфейсу S4 працює протокол GTP.

На рис. 2.3 зображено підключення після хендоверу між технологіями радіодоступу, тобто перехід з'єднання від E-UTRAN до UTRAN/GERAN. В цьому випадку використовуються інтерфейси S3, S4 та S12, котрі описані нижче. З'єднання за допомогою інтерфейсів S5 та SGi залишаються колишніми, але корисне навантаження тепер маршрутизується крізь тунель через інтерфейси S4 та S12. В цей же час сигнальна інформація, котра необхідна для виконання мобільності між технологіями радіодоступу, буде передаватись через інтерфейс S3. Після успішної передачі обслуговування з'єднання, старі канали передачі даних і сигнальних з'єднань S1-U та LTE-Uu будуть видалені.

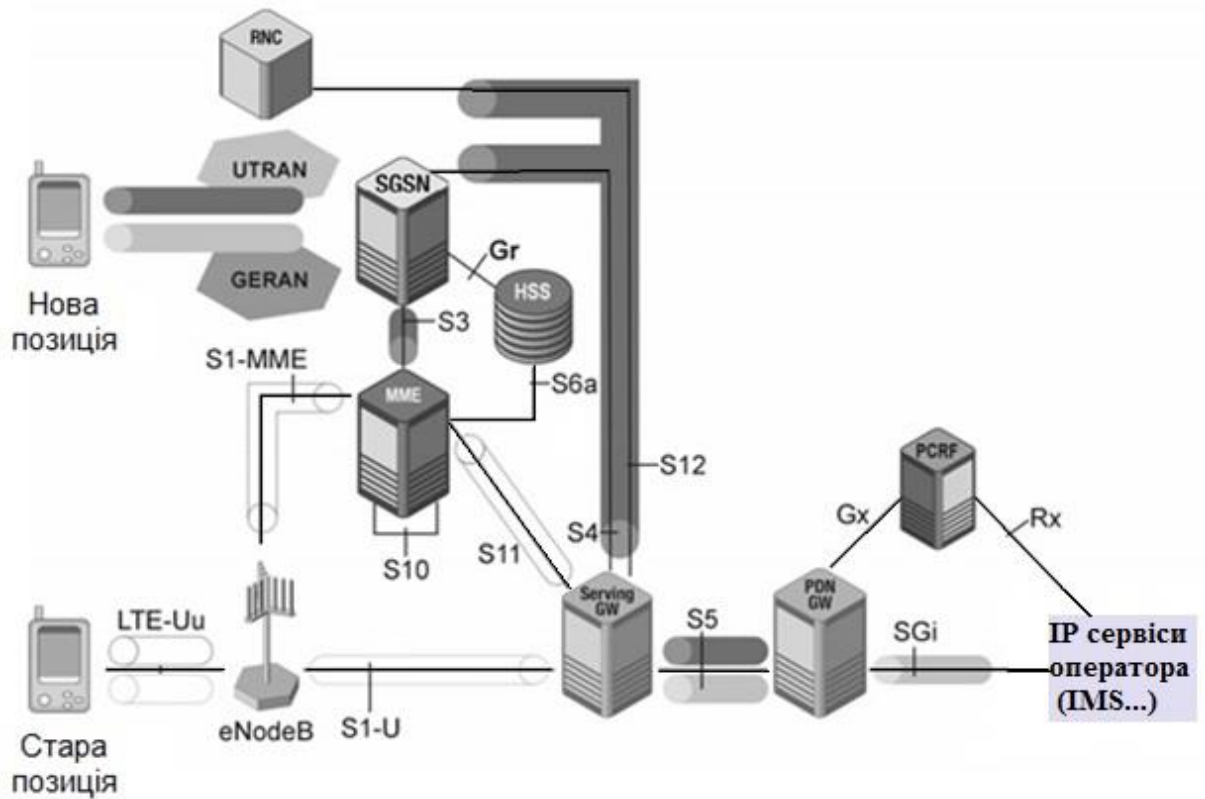


Рисунок 2.3 Підключення після хендоверу між технологіями радіодоступу від E-UTRAN до UTRAN/GERAN

S5 – це інтерфейс між обслуговуючими шлюзами S-GW та пакетними P-GW, що забезпечує встановлення сесій і передачу даних користувачів. Між даними шлюзами встановлюється тунельне з'єднання та використовується протокол GTP, як для користувацької площини, так і для площини управління.

S6a – це інтерфейс між вузлом управління мобільністю MME та домашнім сервером бази даних користувачів HSS. Даний інтерфейс забезпечує автентифікацію і авторизацію користувачів, оновлення даних про їх місцезнаходження. По інтерфейсу S6a використовується протокол DIAMETER.

Gx – це інтерфейс між мережевим елементом застосування політик доступу і тарифікації PCEF вузла P-GW і вузлом управління політиками доступу й тарифікаціями PCRF. Даний інтерфейс забезпечує управління якістю передачі даних і тарифікацією протягом всієї сесії користувача. По

інтерфейсу Gx працює протокол DIAMETER.

S8 – це інтерфейс між обслуговуючим шлюзом S-GW та пакетним шлюзом P-GW, що знаходяться в різних мережах (домашній та візитній). Даний інтерфейс забезпечує управління сесіями і передачу даних користувачів, котрі знаходяться в роумінгу, а також є аналогом інтерфейсу S5. По інтерфейсу S8 працює протокол GTP.

S9 – це інтерфейс між домашнім і візитним PCRF (H-PCRF та V-PCRF), котрий забезпечує управління якістю передачі даних і тарифікацією абонентів, що знаходяться в різних мережах (роумінгу). Наприклад, якщо абонент намагається зареєструватись у візитній мережі, то домашній PCRF повинен передати у візитний PCRF інформацію про передплатений ліміт та необхідні правила для забезпечення належної тарифікації. По інтерфейсу S9 працює протокол GTP.

S10 – це інтерфейс між двома вузлами управління мобільністю MME, котрий забезпечує хендовер зі зміною вузла MME та їхню взаємодію в різних мережах LTE. По інтерфейсу S10 працює протокол площини управління GTP-C.

S11 – це інтерфейс між вузлом управління мобільністю MME і обслуговуючим шлюзом S-GW, котрий забезпечує управління сесіями користувачів. По інтерфейсу S10 працює протокол площини управління GTP-C.

S12 – це інтерфейс між контролером RNC мережі радіодоступу UTRAN і обслуговуючим шлюзом S-GW, котрий забезпечує формування тунелів для передачі даних користувачів об'єднаної мережі LTE/UMTS. По інтерфейсу S12 працює протокол користувацької площини GTP-U.

S13 – це інтерфейс між вузлом управління мобільністю MME та реєстром ідентифікації обладнання (Equipment Identity Register, EIR), котрий забезпечує розпізнавання обладнання абонентського терміналу користувача. По інтерфейсу S13 працює протокол DIAMETER.

SGi – це інтерфейс між пакетним шлюзом P-GW та зовнішньою

мережею комутації пакетів, а також підсистемою IMS (IP Multimedia Subsystem) і сервісними платформами оператора. По інтерфейсу SGi працює протокол мережевого рівня IP.

Rx – це інтерфейс між вузлом управління мережевими політиками і тарифікації PCRF та вузлом, що виконує прикладні функції (Application Function - AF). Він забезпечує застосування кастомізованих політик щодо користувачів. Наприклад, якщо послуги зв'язку надаються в реальному часі, такі як передача голосу по IP (Voice over IP, VoIP), то тарифікація повинна відрізнятись від загальної моделі при передачі даних. По інтерфейсу Rx працює протокол DIAMETER.

На рис. 2.4 зображено базове підключення через E-UTRAN в інші мережі EPC при обслуговуванні абонента в роумінгу. Таке підключення можливе коли, абонент починає використовувати ресурси гостьової мережі. Це може бути зв'язано з втратою покриття зв'язку домашньої мережі. Сигнальне та корисне навантаження проходить по схожому маршруту, як показано на рисунку 2.3. Проте, підключення домашнього S-GW з гостьовим P-GW відбувається по інтерфейсу S8, котрий також, як і інтерфейс S5, працює по протоколу GTP. Єдина відмінність між інтерфейсами полягає в тому, що S8 повинен відповідати більш високим вимогам у відношенні взаємодії, оскільки він забезпечує з'єднання між різними мережами, де відповідно може використовуватись обладнання різних виробників.

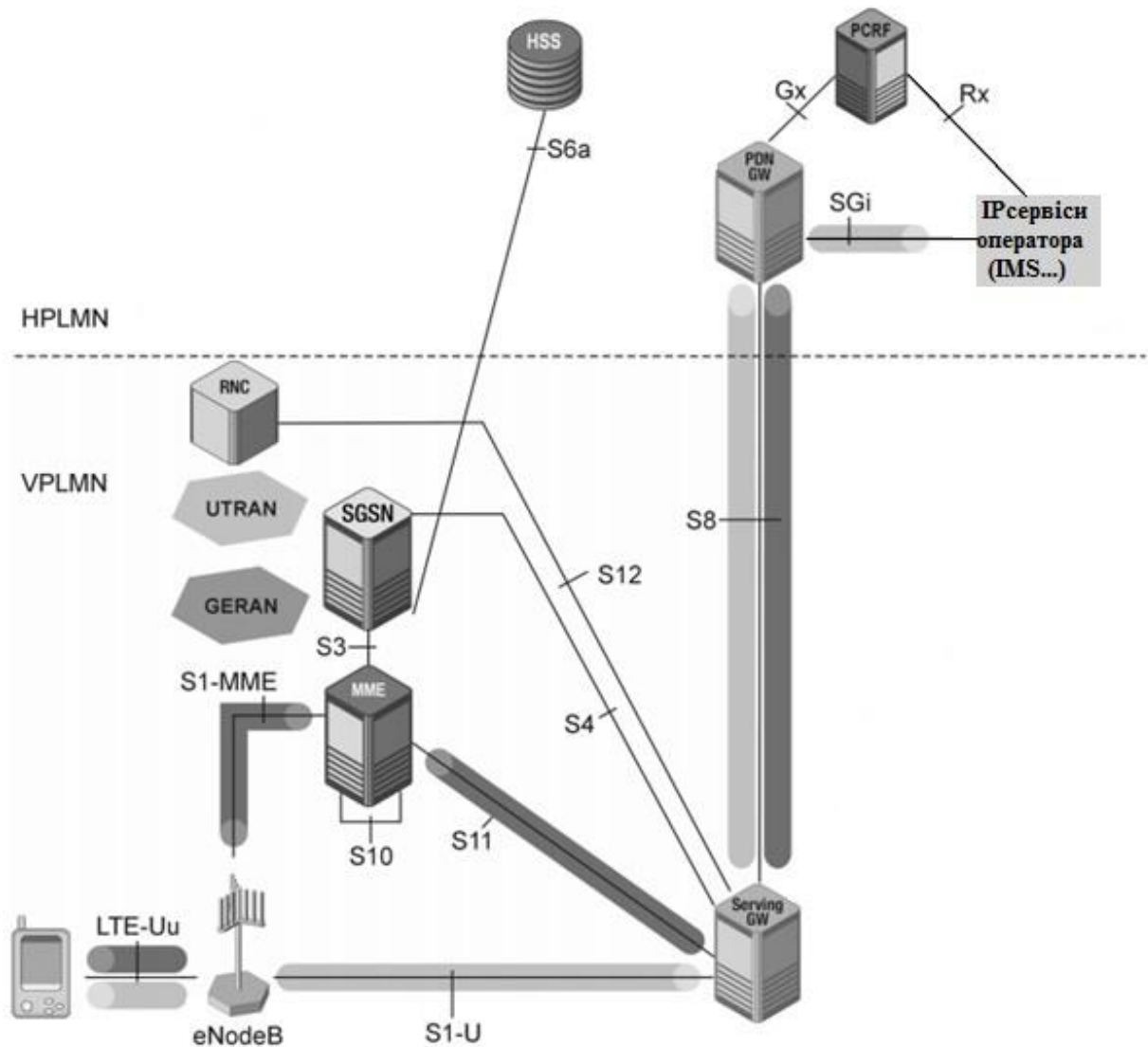


Рисунок 2.4 Підключення через E-UTRAN в інші мережі EPC при обслуговуванні абонента в роумінгу

Основними протоколами, що працюють між вузлами модернізованого ядра EPC є: DIAMETER, GTP та SCTP. Розглянемо детальніше їхнє призначення.

DIAMETER – це протокол, який розроблений для забезпечення основних функцій AAA, а саме: автентифікації, авторизації та обліку. Даний протокол являється модернізованим протоколом RADIUS. В мережах 3G з його допомогою відбувається оцінка послуг передачі даних, а в IMS/LTE протокол є одним з основних управляючих елементів. Особливістю DIAMETER є його розширюваність і можливість створення не тільки

особистих атрибутів, але й додатків. Безпека протоколу забезпечується на транспортному рівні.

GTP – це протокол тунелювання GPRS. Він використовується для інкапсуляції користувацьких даних при проходженні через базову мережу, а також переносить сигнальний трафік окремого канал-носія між різними вузлами мережі. Його основною функцією є створення, модифікація та видалення тунелів для передачі корисного IP-навантаження. Протокол GTP має дві версії: GTP-v1 та GTP-v2. GTP-v1 використовується для GTP-U, тобто для перенесення користувацького трафіку. GTP-v2, в свою чергу, використовується для GTP-C, тобто для перенесення управляючої інформації.

SCTP – (Stream Control Transmission Protocol) це протокол передачі управління потоком. Він працює на транспортному рівні і є аналогом протокола TCP (Transmission Control Protocol). В мережах LTE даний протокол використовується для гарантованої доставки повідомлень між MME та eNodeB. SCTP відноситься до стеку протоколів SIGTRAN (Signaling Transport) і використовується для передачі телекомунікаційної сигналізації по IP. SCTP дозволяє обмінюватись декількома потоками повідомлень по одному з'єднанню. Основні переваги перед протоколом TCP: багатопотоковість, тобто здатність одночасно паралельно передавати по декільком незалежним потокам повідомлень, а також вища безпека [13].

Оскільки мережі LTE працюють лише з комутацією пакетів, то традиційний підхід до передачі голосу, який був у мережах попереднього покоління за допомогою комутації каналів, не може бути реалізованим. Проте, завдяки впровадженню IP-сервісів та додаткового домену IMS (IP Multimedia Subsystem) можливо забезпечити передачу голосу в IP-мережах. Опорним ядром для обробки голосового трафіку, що передається у вигляді IP-пакетів, буде мультимедійна підсистема IMS, що працює на основі протоколу IP. Мобільний термінал перш ніж зареєструватись в ядрі IMS, повинен успішно зареєструватись в ядрі пакетної комутації EPS, щоб

встановити сигнальні лінки між підсистемами та забезпечити передачу управляючої інформації..

2.2 Система IMS, основні протоколи, процедури та принцип надання голосових послуг.

Підсистема IMS створена щоб надавати IP-мультимедійні послуги. Її розробка належить партнерській організації 3GPP. Архітектура та технічні принципи функціонування IMS описані в специфікаціях TS 23.417 [14] і TS 23.517 [15].

IMS - це мультимедійна підсистема мереж четвертого покоління, котра дозволяє організовувати голосові виклики, відеоконференції та інші сервіси в LTE. Основними сигнальними протоколами в ній є SIP (Session Initiation Protocol) та SDP (Session Description Protocol). Передача медіапотоків здійснюється за допомогою протоколу RTP (Real-Time Transport Protocol).

На рис. 2.5 зображено взаємодію підсистеми IMS з пакетним ядром EPC.

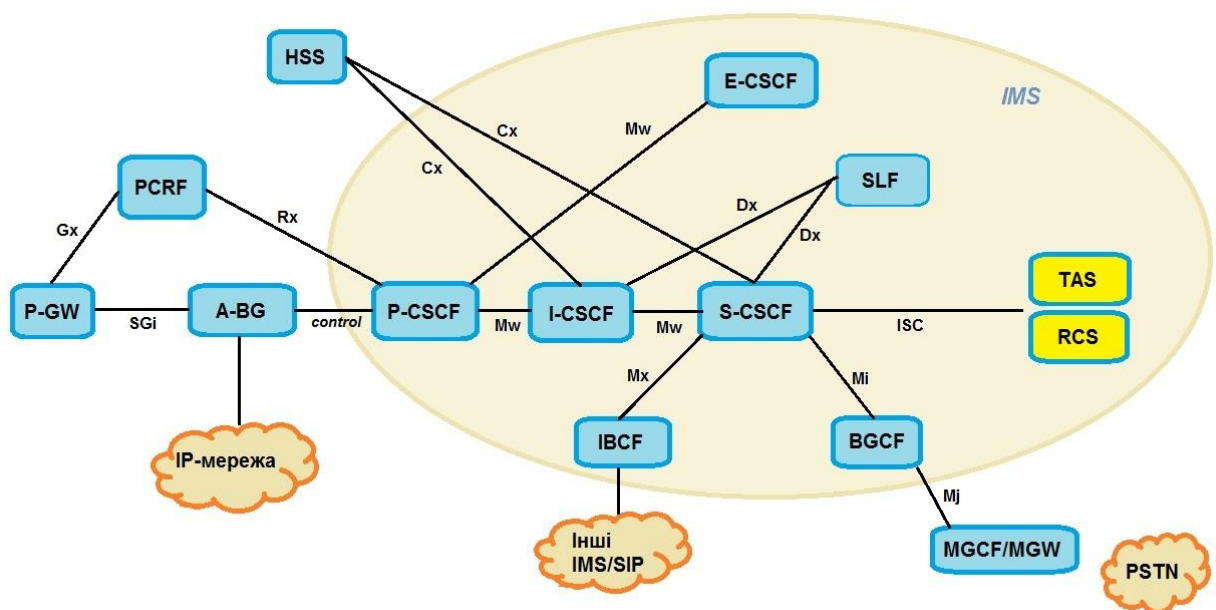


Рисунок 2.5 Взаємодія підсистеми IMS з пакетним ядром EPC

Основним функціональним елементом IMS є функція управління сеансом зв'язку (Call Session Control Function, CSCF). В свою чергу CSCF поділяється на чотири типи:

- P-CSCF (Proxy CSCF), проксі CSCF;
- S-CSCF (Serving CSCF), обслуговуючий CSCF;
- I-CSCF (Interrogating CSCF), запитуючий CSCF;
- E-CSCF (Emergency CSCF), екстрених служб CSCF.

Кожен CSCF виконує свої спеціалізовані задачі. В загальному, елементи CSCF відповідають за SIP-сесію, реєстрацію абонентського терміналу, забезпечують механізм SIP-маршрутизації і реалізують логіку для наступних функцій:

- автентифікація користувача;
- маршрутизація виклику;
- управління створенням детальних записів викликів (Call Detail Records, CDR) в цілях обліку і тарифікації.

Розділення CSCF на окремі функціональні блоки забезпечує розподіл навантаження і надає підвищену надійність за рахунок використання серверів резервного копіювання. В якості протоколу сигналізації використовується SIP, а інтерфейсом підключення між ними виступає Mw. Взаємодія з іншими доменами, використовуючи різні протоколи, здійснюється виділеними елементами, котрі забезпечують трансляцію протоколів. Розглянемо детальніше елементи CSCF.

Першою точкою з'єднання мобільного терміналу в IMS, що зареєстрований в пакетній мережі EPC, є P-CSCF. Вона може знаходитись як у домашній, так і візитній мережі. До основних функцій та задач даного елемента можна віднести:

- SIP компресія, для пришвидшення процедури встановлення сесій;
- контроль цілісності та захист конфіденційності SIP сигналізації завдяки використанню протоколів IPsec і TLS (Transport Layer Security);

- маршрутизація запитів на реєстрацію, отриманих від UE, в I-CSCF;
- маршрутизація SIP повідомлень в S-CSCF;
- маршрутизація запитів та відповідей в UE;
- взаємодія з PCRF;
- виявлення екстреного виклику та передача його на відповідний E-CSCF;
- управління QoS та виділення ресурсів через Rx інтерфейс.

I-CSCF є точкою в мережі оператора для всіх вхідних з'єднань до абонентів даного оператора, а також являється посередником для взаємодії із зовнішніми мережами. До основних функцій та задач даного елементу можна віднести:

- призначення користувачу відповідного S-CSCF, ґрунтуючись на даних, отриманих від HSS;
- забезпечення алгоритму балансування для вибору S-CSCF, використовується у випадку початкової реєстрації користувача;
- маршрутизація SIP повідомлень до S-CSCF;
- трансляція адреси абонента з телефонного формату в SIP URI (SIP Uniform Resource Identifier) з використанням сервера ENUM (E.164 Number Mapping).

S-CSCF є центральною точкою сигнальної площини в домені IMS. Для того, щоб розподілити навантаження і забезпечити високу доступність, в мережі може бути декілька таких елементів. Мобільний термінал, надсилаючи запит на реєстрацію, в підсумку маршрутизується на S-CSCF, котрий у свою чергу ініціює процедуру автентифікації і завантажує профіль користувача з HSS. Після верифікації даних, S-CSCF підтверджує реєстрацію в IMS. До основних функцій та задач даного елементу можна віднести:

- управління сесіями абонентів;
- автентифікація абонентів;
- отримання профайла абонента і початкових критеріїв фільтрації

(Initial Filter Criteria, IFC) від HSS та подальше їх зберігання;

- трансляція адреси абонента з телефонного формату в SIP URI з використанням сервера ENUM;
- взаємодія з програмними серверами (Application server, AS);
- застосування політик оператора;
- маршрутизація викликів у зовнішні мережі, а саме, телефонні (Public Switched Telephone Network, PSTN) та SIP домени.

E-CSCF – це виділений елемент для обробки екстрених викликів (виклики поліції, пожежної служби, швидкої допомоги та інших). Основними задачами є: вибір екстрених контакт-центрів, котрі приймуть виклик, та оптимальна маршрутизація виклику [16].

Шлюз доступу (Access Border Gateway, A-BG) – це компонент, що розмежовує домени EPC та IMS. Таким чином, він для користувачів EPC приховує топологію, адреси і порти, що знаходяться в IMS, такі ж дії виконуються і для користувачів зі сторони IMS. До основних функцій та задач даного елемента можна віднести:

- приховання деталей топології;
- можливість встановлення IPsec/TLS тунелю з IMS клієнтом;
- забезпечення гарантованого проходження користувацького трафіку через IMS ядро;
- забезпечення зручності реалізації тарифікації абонентів.

Домашній сервер абонентів HSS, що є одним з головних вузлів пакетного ядра, виконує схожі функції для мультимедійної підсистеми IMS. Перш за все, HSS виступає, як база даних, де зберігається вся інформація про абонентів. Він взаємодіє з I/S-CSCF через інтерфейс Sx. В базі даних HSS може міститись наступна інформація:

- сервісні профайли з параметрами підписки;
- інформація для ідентифікації та авторизації абонента ;
- інформація про місцезнаходження та IP адреси користувача;
- інформація про логіку обробки викликів з використанням

початкових критеріїв фільтрації IFC.

У випадку, коли в підсистемі IMS використовується декілька серверів HSS, потрібно додатково вводити функціональний елемент SLF (Subscription Locator Function). Він займається пошуком відповідного HSS з даними про конкретного користувача. SLF взаємодіє з I/S-CSCF через інтерфейс Dx, що є аналогом Cx для домашнього серверу користувачів. Функція визначення місцезнаходження підписки SLF не виконує жодної логіки на своїх інтерфейсах, але відповідає запитувачу (requestor) повідомленням REDIRECT (переадресація), вказуючи адресу HSS, що містить відповідь на отриманий запит. Обидва мережеві вузли працюють по протоколу DIAMETER.

TAS (Telephony Application Server) – сервер телефонних додатків, котрий приймає та обробляє повідомлення протоколу SIP, а також визначає яким чином має бути ініційований вихідний виклик. Сервісна логіка TAS забезпечує базові сервіси обробки викликів, а саме: маршрутизацію, встановлення, очікування та перенаправлення, конференц-зв'язок та інші. Він також забезпечує сервісну логіку для звернення до медіасерверів при необхідності відтворення оповіщення та сигналів проходження виклику. Сервер додатків TAS може розміщуватись, або в оператора домашньої мережі користувача, або у сервісного провайдера. До основних функцій TAS можна віднести:

- можливість обробки SIP сесій, отриманих від IMS;
- можливість створення вихідного SIP запиту;
- можливість генерації тарифікаційних даних.

RCS (Rich Communication Services) – це система передачі коротких повідомлень та контактних даних між абонентами мобільного зв'язку. Таким чином, RCS дозволяє здійснювати передачу повідомлень через домен мультимедійної підсистеми IMS за допомогою IP протоколу [17].

BGCF (Breakout Gateway Control Function) – це функція управління шлюзами переривання, що знаходиться на кордоні ядра IMS. Вона забезпечує маршрутизацію викликів між доменом комутації каналів PSTN та мережею

IMS. BGCF приховує порти, що знаходяться в IMS, здійснює маршрутизацію по телефонному номеру, а також обирає відповідний шлюз в домені комутації каналів, через котрий здійснюватиметься взаємодія IP мультимедійної підсистеми та PSTN.

MGCF (Media Gateways Control Function) – функція управління медіашлюзами, котра дозволяє перетворювати кодеки, що використовуються в різних мережах. У випадку, коли MGCF знаходиться в голосовому домені (CS Network), вона може перетворювати сигнальні повідомлення, що передаються по протоколу SIP, у відповідні повідомлення протоколу ISUP (ISDN User Part), котрий використовується в традиційних системах.

MGW (Media Gateway) – медіашлюз, що знаходиться на кордоні між мережею IMS, котра працює на основі протоколу SIP та традиційною мережею PSTN. Він здійснює трансляцію даних між різними мережами використовуючи узгоджені кодеки [18].

IBCF (Interconnect Border Control Function) – функція контролю з'єднань між різними мережами, що забезпечує безпеку сигнальної інформації [19]. Детальні принципи побудови IBCF були розроблені партнерською організацією 3GPP та описані в технічній специфікації TS 29.238 [20].

До головних переваг IP мультимедійної підсистеми IMS можна віднести:

- забезпечення взаємодії різних типів мереж;
- забезпечення якості надання послуг (QoS);
- можливість розробки та впровадження нових послуг;
- висока масштабованість;
- забезпечення точної тарифікації;
- низькі витрати на експлуатацію.

Архітектура IMS поділяється на три горизонтальні рівні, а саме:

- транспортний рівень, котрий організовує сеанс зв'язку за допомогою протоколу SIP та забезпечує транспортні послуги з

конвертацією голосу із аналогового або цифрового сигналу в IP-пакети, використовуючи протокол RTP;

- рівень управління викликами та сеансами зв'язку;
- прикладний рівень або рівень послуг, що містить набір серверів додатків (Application Servers, AS).

На рис. 2.6 зображено розподіл архітектури IMS на горизонтальні рівні.

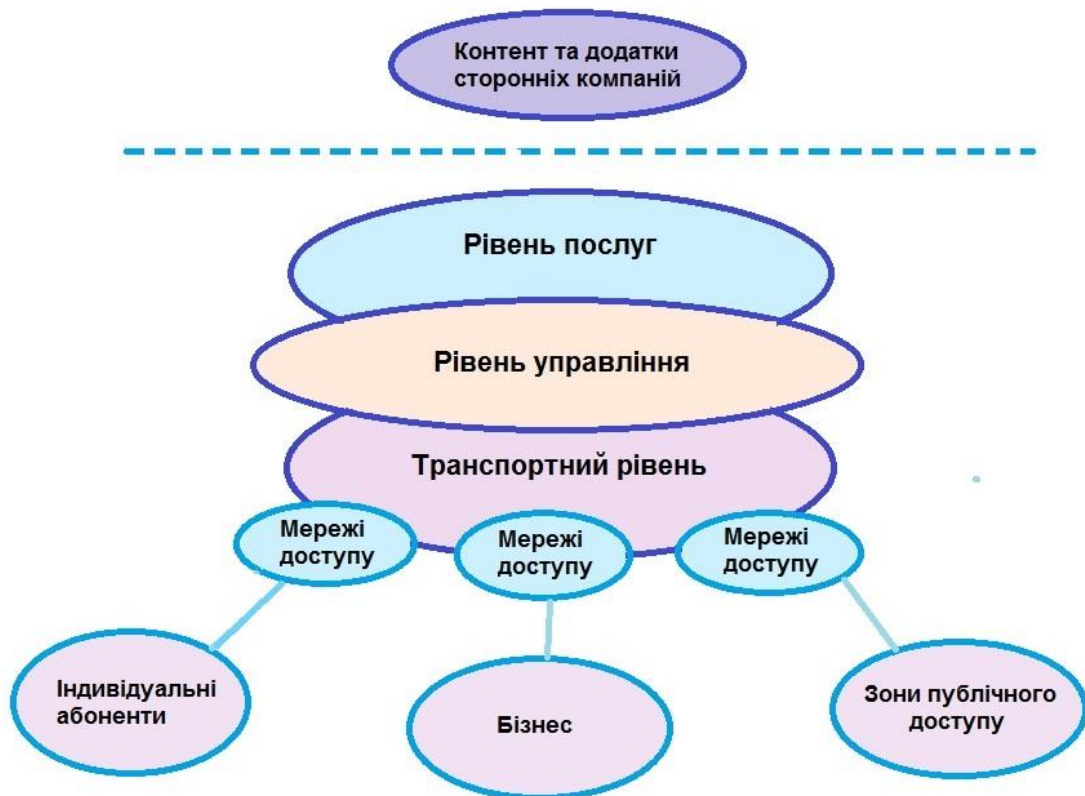


Рисунок 2.6 Розподіл архітектури IMS на горизонтальні рівні

Основними протоколами, що використовуються в архітектурі підсистеми IMS є:

- протокол ініціації (управління) сеансом – SIP;
- протокол опису сеансу – SDP;
- транспортні медіа протоколи, а саме RTP та RTCP;
- протоколи управління медіа – MEGACO/H.248;
- протокол автентифікації DIAMETER [21].

Розглянемо детальніше дані протоколи.

SIP (Session Initiation Protocol) – це протокол ініціювання сеансу, що працює на прикладному рівні. Він призначений для встановлення, зміни та завершення користувацького інтернет-сеансу. Прикладом використання може бути: IP-телефонія, багатокористувацькі конференції (котрі включають в себе голос, відео та дані), чати миттєвого обміну повідомленнями і онлайн-ігри. SIP є текстовим та високомасштабованим протоколом. Основні принципи побудови протоколу SIP були розроблені відкритим міжнародним співтовариством проектувальників IETF (Internet Engineering Task Force) і опубліковані в стандарті RFC 3261 (Request For Comment) [22]. Також SIP являється головним протоколом в архітектурі IMS.

Протокол SIP має клієнт-серверну архітектуру. Клієнт надсилає запити на сервер за допомогою спеціальних повідомлень. Сервер, в свою чергу, приймає і обробляє запити, потім надсилає відповідь клієнту, в котрій міститься інформація про успішне або невдале виконання запиту.

Основними повідомленнями протоколу SIP під час створення та завершення активної сесії зв'язку є:

- REGISTER – повідомлення, яке надає інформацію про поточне місцезнаходження користувача;
- INVITE – повідомлення, що пропонує іншому користувачу вступити в сеанс зв'язку. В ньому може міститись інформація яка описує даний сеанс, а саме: використовувані кодеки та IP-адреса;
- ACK – повідомлення-підтвердження зі сторони запитувача на встановлення сеансу зв'язку. В ньому можуть передаватись остаточні параметри сеансу зв'язку;
- CANCEL – повідомлення, що відміняє передані раніше запити, на які ще не було отримано відповідь;
- BYE – повідомлення, яке сигналізує про завершення сеансу зв'язку;
- OPTIONS – повідомлення для запиту про функціональні можливості терміналу (наприклад, чи підтримується певний тип медіа).

Також під час відправлення відповідей на запити застосовуються спеціальні класи. Відповіді кодуються трьохзначним числом, де перша цифра вказує на її клас, а інші дві ідентифікують конкретну відповідь в класі. Прикладами можуть бути:

- 1xx – інформаційні відповіді;
- 2xx – успішне закінчення запиту;
- 3xx – інформація про зміну місцезнаходження користувача;
- 4xx – інформація, що сигналізує про помилку;
- 5xx – інформація, що сигналізує про помилку на сервері;
- 6xx – інформація, про неможливість прийняття виклику.

Розглянемо спрощений приклад встановлення SIP сесії між двома користувачами на рис. 2.7. На першому кроці сторона А надсилає повідомлення INVITE на Proxy сервер, котрий перенаправляє його на сторону Б. У випадку, коли сторона Б готова прийняти запрошення на встановлення сесії зв'язку, вона направляє повідомлення 200OK. Потім сторона А підтверджує з'єднання повідомленням ACK і після цього сесія вважається успішно встановленою [23].

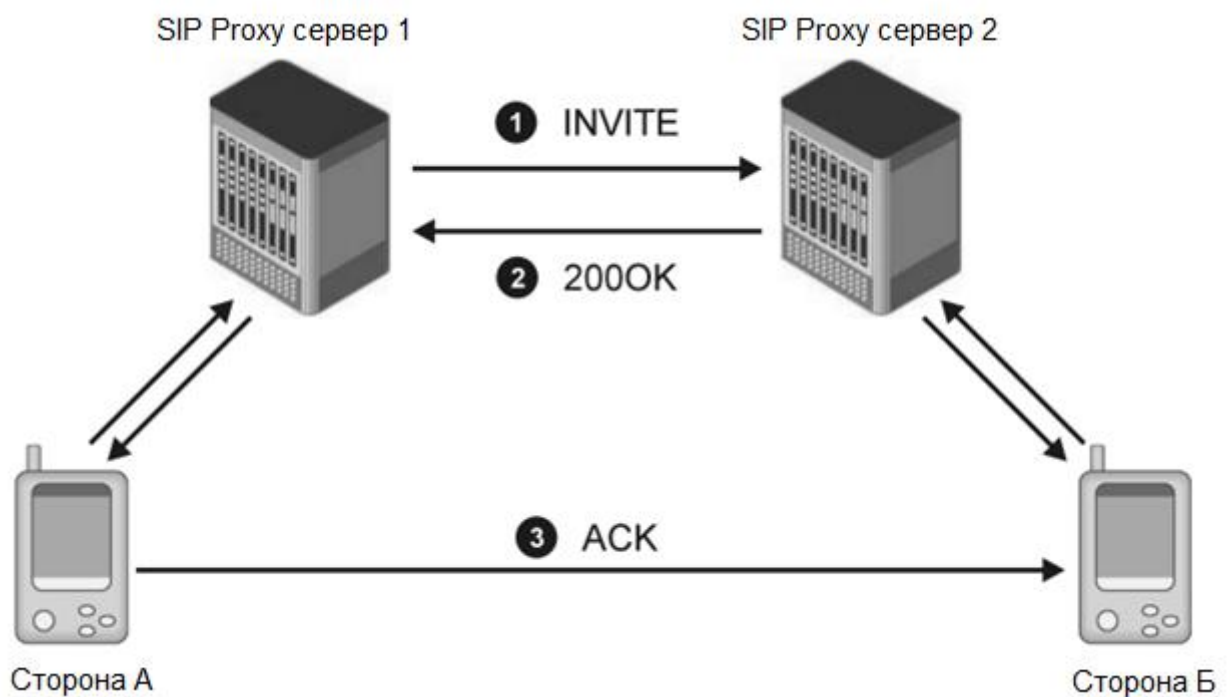


Рисунок 2.7 SIP сесія між двома користувачами

SDP (Session Description Protocol) – це мережевий протокол прикладного рівня, котрий призначений для опису сеансів передачі поточкових даних. Перед встановленням сеансу зв'язку між користувачами, потрібно узгодити тип і правила кодування інформації. SDP може містити всю необхідну інформацію про користувачів і принципи з'єднання, а саме: типи використовуваних медіа потоків, номери портів, IP-адреси, кодеки та іншу інформацію. Сесія SDP може підтримувати декілька потоків даних. Даний протокол широко використовується в IP мультимедійній підсистемі, а також він доповнює процес управління викликом, виконуючи функції опису параметрів SIP-сесій.

RTP (Real-Time Transport Protocol) – це протокол прикладного рівня, котрий передає аудіо- та відеодані через IP мережі в режимі реального часу. В якості транспортного протоколу він зазвичай використовує UDP (User Datagram Protocol), що працює без встановлення з'єднань. Даний протокол дозволяє одночасно обмінюватися даними в багатоадресній передачі. Він реалізує розпізнання типу трафіку, нумерацію послідовності пакетів та контроль передачі.

Протокол RTP працює разом з RTCP (Real-Time Transport Control Protocol), котрий використовується для передачі службової інформації про якість послуг та виникненні перевантажень. RTCP також слугує для контролю параметрів активного каналу зв'язку.

Протоколи управління медіа MEGACO/H.248 забезпечують взаємодію шлюзів, що перетворюють голосовий трафік мереж з комутацією каналів в пакетний трафік мереж з комутацією пакетів. Також вони дозволяють відокремлювати управління викликом від медіа потоку [24].

Оскільки мережі четвертого покоління не передбачають наявності домену з комутацією каналів, то традиційний метод передачі голосу не може бути застосований. У випадку, коли мобільний термінал зареєстрований в пакетному ядрі мережі LTE, може використовуватись процедура CS-FallBack (Circuit Switched FallBack). Вона реалізовує функцію переходу UE від мережі

4G в мережі 3G/2G. CS-FallBack виконується в декількох випадках, наприклад: коли користувач намагається здійснити голосовий виклик (відбувається перереєстрація мобільного терміну в мережі попереднього покоління) або коли йому надходить голосовий виклик. Технічний принцип побудови CS-FallBack розроблений партнерською організацією 3GPP та описаний в специфікації TS 23.272 [25]. Таким чином, блок управління мобільністю MME за допомогою інтерфейсу SGs передає обслуговування користувачів в центр мобільної комутації (Mobile Switching Center, MSC), котрий працює в мережах з підтримкою голосового домену.

На рис. 2.8 зображено спрощену схему архітектури мережі LTE при організації процедури CS-FallBack.

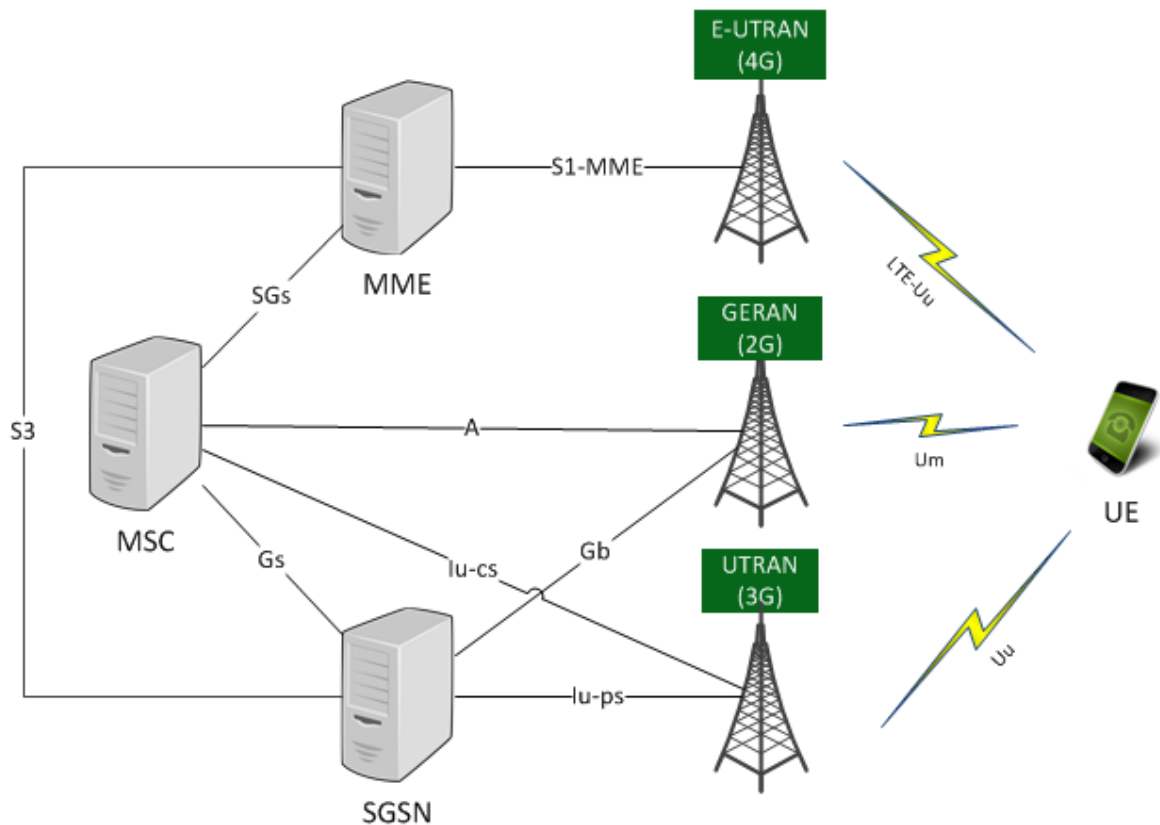


Рисунок 2.8 Архітектура мережі LTE при організації CS-FallBack

Впровадження IP мультимедійної підсистеми IMS дозволяє реалізувати технологію передачі голосу в мережі LTE (Voice over LTE, VoLTE). Тоді голосовий трафік буде передаватись на основі протоколу IP. До основних

переваг технології VoLTE можна віднести:

- висока швидкість з'єднання мобільних пристроїв, завдяки відсутності процедури CS-FallBack;
- висока якість голосу (HD-Voice);
- можливість неперервного використання мобільного інтернету 4G при телефонній розмові;
- низькі витрати заряду акумулятора мобільного пристрою.

Таким чином впровадження технології VoLTE забезпечує міграцію голосового трафіку в мережі 4G

На рис. 2.9 зображено поетапну міграцію трафіку з мереж 3G/2G в LTE.

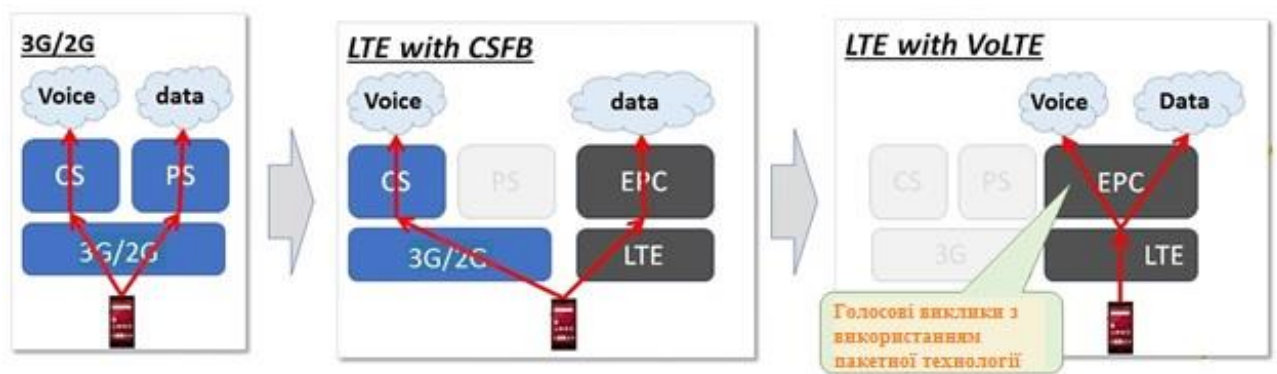


Рисунок 2.9 Міграція трафіку з мереж 3G/2G в LTE

Голосовий потік є чутливим до характеристик передачі (затримка, джиттер). Для забезпечення якості, в мережах четвертого покоління передбачено підтримка QoS (Quality of Service). В залежності від вимог QoS, всі види послуг поділені на 9 класів і кожному класу призначений ідентифікатор QCI (QoS Class Identifier). В свою чергу, наскрізні канали для передачі трафіку поділені на дві групи в залежності від типу виділеного ресурсу, а саме: з гарантованою швидкістю передачі (Guaranteed Bit Rate, GBR) та з негарантованою швидкістю передачі Non-GBR. В табл. 2.1 наведено якісні показники для основних видів надання послуг в мережах LTE.

Таблиця 2.1 Якість обслуговування в мережах LTE

QCI	Тип	Пріоритет	Допустима затримка, мс	Допустимі втрати	Приклад
1	GBR	2	100	10^{-2}	VoLTE виклик
2		4	150	10^{-3}	Відео виклик
3		5	300	10^{-6}	Онлайн ігри
4		3	50	10^{-3}	«Стрім» відео
5	Non-GBR	1	100	10^{-6}	IMS
6		7	100	10^{-3}	Електронна пошта, чат
7		6	300	10^{-6}	Голосові, відео, інтерактивні ігри
8		8	300	10^{-6}	Електронна пошта, чат
9		9	300	10^{-6}	

Для того, щоб організувати технологію VoLTE потрібна підтримка двох QCI: 1 та 5. QCI 1 призначений для передачі голосу, а QCI 5 – для сигнальних IMS повідомлень. З'єднання по QCI 5 забезпечує передачу керуючих повідомлень для створення та видалення голосових сесій. При цьому використовується протокол SIP. Через з'єднання по QCI 1 голосові дані передаються з використанням стека протоколів RTP/UDP/IP [26].

Архітектура IMS дозволяє організувати процедуру безперервного голосового виклику (Single Radio Voice Call Continuity, SRVCC). У випадку, коли мобільний термінал, що має активну голосову сесію в ядрі IMS, раптово втрачає покриття LTE, то відбувається перереєстрація його в мережі 3G/2G. Блок управління мобільністю MME сигналізує по інтерфейсу Sv в центр мобільної комутації MSC про необхідність негайної передачі обслуговування абонента. Таким чином, забезпечується «гладка» передача голосового виклику з 4G в мережі попереднього покоління. Технічні принципи побудови процедури SRVCC розроблені партнерською організацією 3GPP та описані в специфікації TS 23.216 [27].

На рис. 2.10 зображено взаємодію блока управління мобільністю MME, під час процедури SRVCC, з центром мобільної комутації MSC за допомогою інтерфейсу Sv.

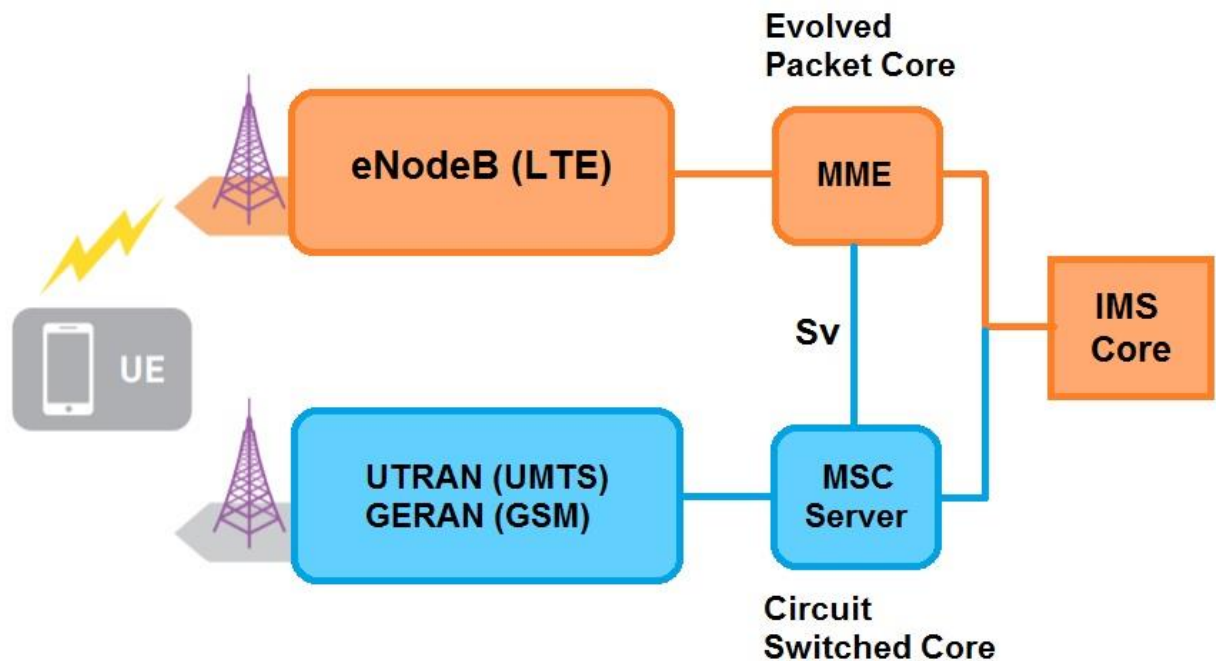


Рисунок 2.10 Взаємодія MME з MSC під час процедури SRVCC

2.3 Організація управління «дзвінками» в мережі LTE

Організація управління «дзвінками» в мережі LTE реалізується завдяки протоколу SIP. Він забезпечує адресацію користувачів, встановлення з'єднання між ними та взаємодію з іншими мережами. Розглянемо основні механізми протоколу SIP в управлінні голосових сесій.

Важливим аспектом для ідентифікації абонентів в мережі під час реєстрації та здійснення дзвінків є адресація. Завдяки тому, що SIP є текстовим протоколом, він може використовувати, для забезпечення мобільності користувачів та взаємодії з існуючими додатками IP-мереж, адресу подібну до адреси електронної пошти. Існує 2 основних види адресації: SIP URI та TEL URI.

SIP URI є основним типом адресації. Адреса абонента складається з двох частин. У першій частині міститься ім'я користувача, що зареєстрований в домені або стандартизований міжнародним союзом електрозв'язку, телефонний номер у форматі номерного плану E.164. У другій частині міститься ім'я домену або IP-адреса. Прикладами можуть

бути:

- Ivanov@youtube.com;
- Ivanov@192.168.0.1;
- +380638100624@192.168.0.1;
- +380638100624@youtube.com.

Оскільки під назвою домену може знаходитись велика кількість IP-адрес, то перш, ніж здійснити виклик на вказаний домен, потрібно запросити відповідну IP-адресу. Для цього запит направляється в базу даних DNS (Domain Name System).

Іншим форматом адресації є TEL URI (телефонний формат адреси). У цьому випадку застосовується звичайний номер формату E.164. Проте, оскільки архітектура LTE та протокол SIP побудовані на основі IP, то використовують спеціальну базу даних ENUM (E.164 Number Mapping). Вона відправляє необхідну IP-адресу на запит телефонного номеру.

Не менш важливим в організації управління дзвінками є процедура обміну повідомлень за допомогою протоколу SIP (Call Flow). Завдяки записам трейсів можна виявити несправності в однієї зі сторін ініціювання сесії та виконати певні дії для того, щоб наступні виклики були успішними. Розглянемо приклад базового Call Flow на рис. 2.11 та нижче приведений детальний опис повідомлень при здійсненні голосової сесії.

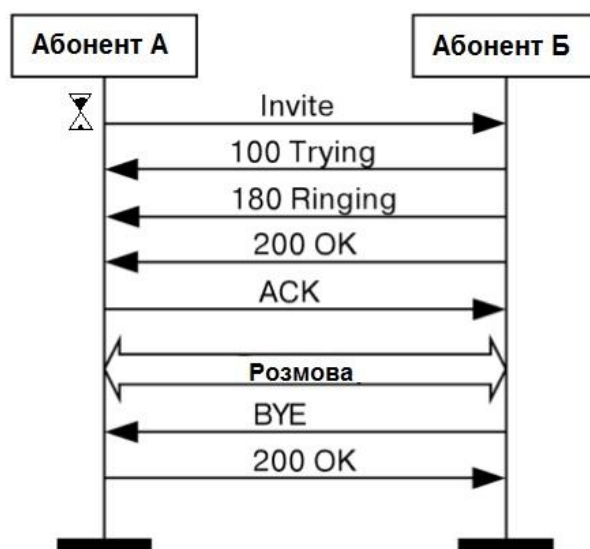


Рисунок 2.11 Базовий Call Flow

- 1) Абонент А надсилає повідомлення «Invite» і таким чином запрошує абонента Б вступити в сеанс зв'язку. За допомогою протоколу SDP, відправляється інформація про обраний тип сесії та підтримувані кодеки, порт і IP-адресу відправника;
- 2) Після відправлення «Invite», вмикається таймер, котрий вказує на час відправки запрошення. Для зупинки таймеру, зі сторони Б відправляється повідомлення «100Trying» (воно зупиняє подальші надсилання «Invite»);
- 3) У випадку, коли абонент Б вільний та має технічні можливості прийняти дзвінок, він надсилає повідомлення «180Ringing». Тоді відбувається контроль посилки виклику;
- 4) Коли абонент Б знімає слухавку (приймає виклик), то він надсилає абоненту А повідомлення «200OK». У ньому міститься інформація про абонента Б (порт, IP-адреса та вибраний кодек із раніше запропонованих);
- 5) Для остаточного встановлення сеансу зв'язку, абонент А надсилає підтвердження «ACK». Воно сигналізує про отримання попереднього повідомлення «200OK». Після цього між абонентами встановлюється з'єднання і за допомогою протоколу RTP відбувається обмін голосовими потоками;
- 6) У випадку, коли абонент Б кладе слухавку, то відправляється повідомлення «BYE». Після цього зі сторони А надходить підтвердження «200OK» і ресурси мережі звільняються.

Для того, щоб забезпечити взаємодію IP-мереж з TDM-мережами, що використовують спільноканальну сигналізацію №7 (Signaling System №7, SS7), були розроблені модифікації протоколу SIP для телефонії. Існує дві версії: SIP-T (SIP for Telephones) та SIP-I (SIP Internetworking). Різниця версій полягає в тому, що SIP-I належить розробці міжнародного союзу електрозв'язку ІТУ-Т, а SIP-T – міжнародного співтовариства проектувальників ІETF. Головною задачею даних модифікацій є «прозора»

передача повідомлень ISUP (ISDN User Part), що використовуються в спільноканальній сигналізації №7, по IP-мережам. Таким чином, сигнальні повідомлення SS7 інкапсулюються в тіло повідомлення SIP, що гарантує передачу необхідних параметрів абонента (наприклад, категорія в мережі). Також можлива трансляція, коли параметри протоколу ISUP транслуються в аналогічні параметри SIP не використовуючи при цьому інкапсуляцію [28].

2.4 Управління доступом в мережу

Обов'язковим критерієм доступу мобільних терміналів у пакетне ядро EPC мережі LTE є наявність у них відповідної USIM-карти (Universal Subscriber Identity Module). Це розширений стандарт SIM-карти (Subscriber Identity Module), котрий прийнятий в рамках LTE партнерською організацією 3GPP та описаний в технічній специфікації TS 31.102 [29]. USIM-карта зберігає в собі інформацію про абонента (підключені послуги, заборонені сервіси, баланс), телефонну книгу, алгоритми і ключі ідентифікації та алгоритми для взаємодії з мережами попереднього покоління. Основними перевагами модернізованого модулю ідентифікації абонента USIM над SIM, що використовується в 3G/2G мережах є:

- збільшена внутрішня пам'ять;
- краща адаптація до роботи з мультимедійними сервісами;
- підтримка більш досконалих стандартів криптографічного захисту;
- можливість зберігання додатків у внутрішній пам'яті модулю.

Під час здійснення доступу UE в мережу LTE, вузол управління мобільністю MME виділяє глобальний унікальний тимчасовий ідентифікатор (Globally Unique Temporary Identity, GUTI) для кожного користувацького терміналу. Дана процедура виконується для того, щоб уникнути багаторазової передачі постійного ідентифікатору абонента (International Mobile Subscriber Identity, IMSI) по радіоканалу. В свою чергу, це дозволяє забезпечити належний рівень безпеки користувацьких даних. У випадку,

коли абонент здійснює першу реєстрацію в пакетній мережі LTE, IMSI перевіряється за допомогою сигналізації функціонального рівня мережі без доступу (Non-Access Stratum, NAS).

Глобальний унікальний тимчасовий ідентифікатор GUTI дозволяє також ідентифікувати MME та мережу, в котрій зареєстрований мобільний термінал. GUTI може використовуватись мережею для унікальної ідентифікації кожного UE під час сигнальних з'єднань. Він складається з двох основних компонентів:

- глобальний унікальний ідентифікатор вузла MME (GUMMEI), котрий однозначно ідентифікує MME, що виділив GUTI;
- тимчасовий ідентифікатор мобільних абонентів (MME Temporary Mobile Subscriber Identity, M-TMSI), котрий однозначно ідентифікує UE в MME, що виділив GUTI.

Ідентифікатор GUMMEI формується за допомогою ідентифікаторів мережі мобільного оператора (Public Land Mobile Network, PLMN), а саме: мобільного коду країни (Mobile Country Code, MCC), коду мобільної мережі (Mobile Network Code, MNC) та ідентифікатора вузла управління мобільністю (груповий ідентифікатор MME Group ID і код вузла MME Code). Призначення MME Code – забезпечити унікальність вузла MME в межах зони його пула. В свою чергу, MME Group ID використовується для ідентифікації різних груп MME.

Існує також коротша форма GUTI, що має назву S-TMSI (System Architecture Evolution TMSI). Вона використовується для ідентифікації мобільного терміналу по радіоканалу та є частиною запиту для з'єднання по протоколу управління радіоресурсами (Radio Resource Control, RRC). S-TMSI містить в собі ідентифікатори MMEC та M-TMSI. Оскільки зони обслуговування вузлів управління мобільністю MME можуть перетинатись, то використовують різні унікальні коди MMEC, що ідентифікують окремі MME.

На рис. 2.12 зображено структуру ідентифікаторів GUTI та S-TMSI.

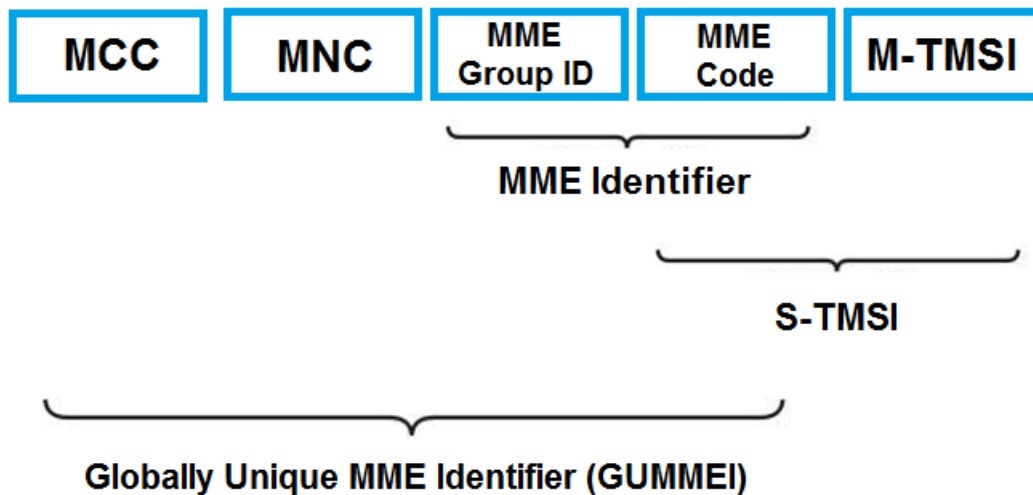


Рисунок 2.12 Структура ідентифікаторів GUTI та S-TMSI

Після того, як мобільний термінал виконав процедуру Attach (прикріплення) до базової станції eNodeB та встановив радіозв'язок, йому необхідно зареєструватись в опорній мережі EPC. Взаємодія UE з блоком управління мобільністю MME виконується за допомогою функціонального рівня без доступу NAS. Він використовується для управління встановленням сеансів зв'язку, автентифікації та забезпечення мобільності користувацьких терміналів. NAS дозволяє обмінюватись сигнальними повідомленнями між UE та елементами опорної мережі. Принципи функціонування NAS описані в технічній специфікації TS 24.301 [30]. Ядро рівня без доступу NAS складається з наступних модулів:

- управління сеансами (EPC Session Management, ESM), котрий включає в себе встановлення, зміну та завершення сеансів, а також узгодження якості обслуговування;
- управління з'єднаннями (EPC Connection Management, ECM), котрий використовується для встановлення з'єднання між UE та MME або для передачі коротких повідомлень;
- управління безпекою, що є додатковим функціоналом NAS для забезпечення цілісності і шифрування сигнальних повідомлень, котрі передаються в мережі під час реєстрації користувача.

Коли процедура реєстрації мобільного терміналу в пакетному ядрі EPC

завершується успішно, то для UE в MME зберігається контекст (необхідні дані про абонента для доступу в пакетну мережу). Також між UE та пакетним шлюзом P-GW встановлюється канал передачі по замовчуванню і призначається йому IP-адреса. Після того, як мобільний термінал отримав IP-з'єднання, він може почати використовувати інтернет-послуги на основі IP або послуги мультимедійної підсистеми IMS, якщо у нього є відповідні підписки [31].

На рис. 2.13 зображено поетапний обмін сигнальних повідомлень за допомогою NAS при реєстрації UE в мережі LTE та наведений детальний опис процедури нижче.

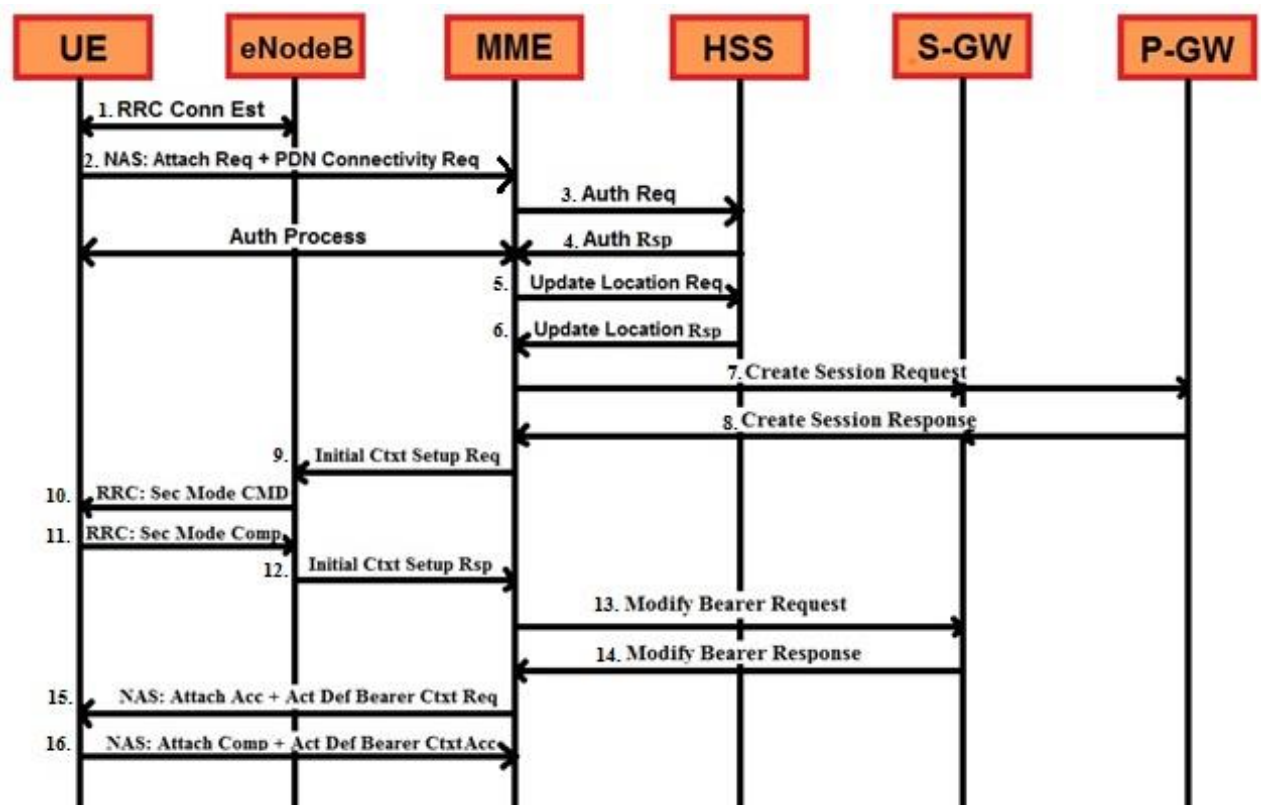


Рисунок 2.13 Поетапний обмін сигнальних повідомлень при реєстрації UE в мережі LTE

- 1) мобільний термінал встановлює RRC-з'єднання з eNodeB;
- 2) UE надсилає разом запити в MME на реєстрацію «Attach Request» та для пакетного підключення «PDN Connectivity Request». В рамках цього, eNodeB встановлює логічне з'єднання по інтерфейсу S1 з

MME;

- 3) Блок управління мобільності MME надсилає в домашній сервер абонентів запит на автентифікацію «Authentication Request»;
- 4) HSS взаємодіє з UE та MME, обмінюючись необхідними ключами для встановлення автентифікації абонента в мережі;
- 5) MME за допомогою протоколу DIAMETER відправляє запит «Update Location Request» до HSS. Таким чином, в домашньому сервері абонентів встановлюється поточне місцезнаходження абонента;
- 6) HSS відправляє відповідь до MME «Update Location Response», в якій міститься підтвердження про оновлення місцезнаходження та профайл абонента;
- 7) MME надсилає повідомлення на створення сесії «Create Session Request». S-GW встановлює GTP-тунель з P-GW та запрошує виділити IP-адресу для UE;
- 8) S-GW отримує відповідь від P-GW «Create Session Response» та відправляє її на MME;
- 9) MME надсилає запит «Initial Context Setup Request», щоб встановити канал зв'язку між eNodeB та S-GW;
- 10) eNodeB встановлює параметри безпеки в UE за допомогою повідомлення «Security Mode Command Procedure»;
- 11) UE завершує встановлення параметрів безпеки та надсилає повідомлення «Security Mode Complete Message» до eNodeB. Після цього всі повідомлення, якими обмінюються UE та eNodeB по радіоінтерфейсу, шифруються і цілісно захищені;
- 12) eNodeB надсилає відповідь до MME «Initial Context Setup Response»;
- 13) MME надсилає запит до S-GW «Modify Bearer Request» на зміну GTP-каналу, щоб оновити ідентифікатор тунеля з eNodeB;
- 14) S-GW надсилає відповідь на MME «Modify Bearer Response», в

котрій міститься інформація про успішне оновлення ідентифікатора тунелю;

- 15) MME надсилає повідомлення-підтвердження до UE про закінчення реєстрації в мережі та запит на активацію каналу за замовчуванням «Attach Accept and Activate Default Bearer Context Request» з використанням NAS;
- 16) UE надсилає підтвердження до MME та активує канал за замовчуванням «Attach Complete and Activate Default Bearer Context Accept». Після цього реєстрацію мобільного терміналу в пакетній мережі LTE вважається успішно завершено [32].

2.5 Забезпечення безпеки в мережі

Мережа LTE характеризується підвищеним рівнем безпеки у порівнянні з мережами попереднього покоління. Перш за все, це досягається завдяки новим механізмам шифрування та захисту цілісності сигнальних повідомлень. Застосування рівня без доступу NAS у мережах LTE призводить до подвійного шифрування. Таким чином, зашифровані повідомлення на транспортному рівні RRC проходять повторне шифрування на рівні NAS. Також важливим нововведенням в архітектурі LTE є використання протоколу безпеки IPsec. За його допомогою гарантується безпечне транспортування користувацького та управляючого IP-трафіку між мережею радіодоступу E-UTRAN та опорним ядром EPC по інтерфейсу S1.

Оскільки IMSI є постійним ідентифікатором, то його передачу по радіоінтерфейсу зводять до мінімуму. Замість IMSI використовують глобальний унікальний тимчасовий ідентифікатор GUTI. Він присвоюється UE в ході реєстрації в мережі та може періодично змінюватись.

Під час активації мобільного пристрою або ініціації процедури реєстрації, здійснюється автентифікація UE та узгодження спеціальних ключів (Authentication and Key Agreement, AKA). Це дозволяє провести

валідацію абонентів та надати їм санкціонований доступ до сервісів і послуг на які вони підписані. Процедура узгодження спеціальних ключів АКА складається з двох етапів. Спочатку HSS генерує вектори автентифікації (RAND, AUTN, XRES, K_{ASME}) і направляє їх до MME. На другому етапі MME обирає один з векторів та використовує його для взаємної автентифікації з UE.

Об'єкт управління безпекою доступу (Access Security Management Entity, ASME) – це об'єкт, котрий приймає ключі верхнього рівня від HSS для використання в мережі доступу. Роль ASME виконує MME, а K_{ASME} слугує ключем верхнього рівня та використовується в мережі доступу. Після взаємної автентифікації UE та MME отримують можливість спільно використовувати K_{ASME} .

Для того, щоб зрозуміти як працює загальна концепція безпеки в LTE, розглянемо на рис. 2.14 ієрархію ключів безпеки, котра запропонована організацією 3GPP в технічній специфікації TS 33.401 [33]. Дана ієрархія включає в себе наступні ключі: K_{eNB} , K_{NASint} , K_{NASenc} , K_{UPenc} , K_{RRCint} , K_{RRCenc} .

K_{eNB} – це ключ, отриманий користувацьким обладнанням і блоком управління мобільністю з ключа управління безпекою доступу K_{ASME} . K_{eNB} використовується тільки для встановлення ключів для передачі трафіку RRC та користувацької площини UP або для здійснення хендверу між базовими станціями.

Ключі для трафіку NAS:

- K_{NASint} – це ключ, котрий використовується тільки для захисту трафіку NAS з визначеним алгоритмом цілісності. K_{NASint} отримують UE та MME з ключа управління безпекою доступу K_{ASME} ;
- K_{NASenc} – це ключ, котрий використовується тільки для захисту трафіку NAS за допомогою визначеного алгоритму шифрування. K_{NASenc} отримують UE та MME з ключа управління безпекою доступу K_{ASME} .

K_{UPenc} – це ключ, котрий використовується тільки для захисту

користувачького трафіку за допомогою визначеного алгоритму шифрування.

K_{UPenc} отримують UE та eNB з ключа K_{eNB} .

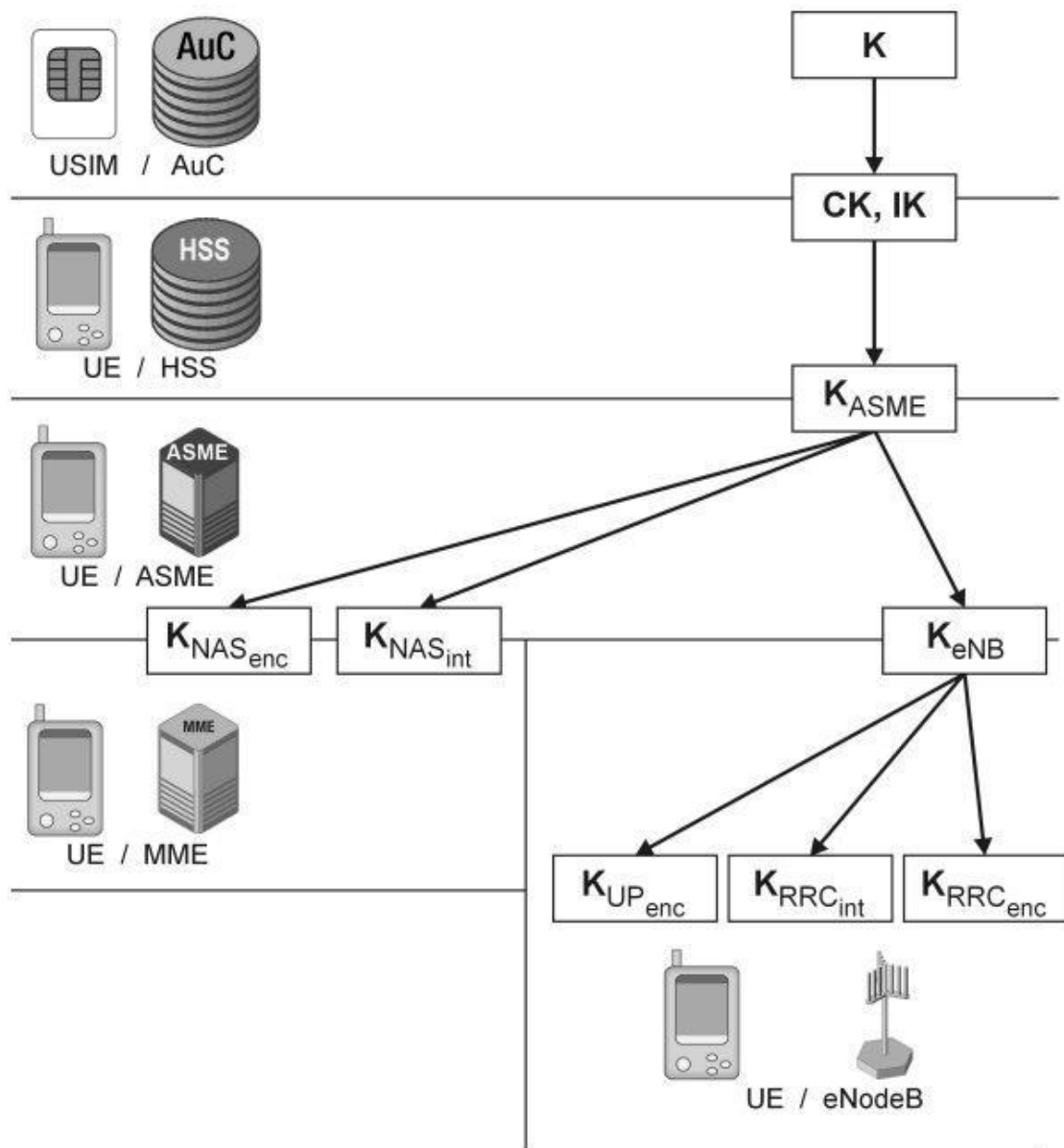


Рисунок 2.14 Ієрархія ключів безпеки в мережі LTE

Ключі для трафіку RRC:

- K_{RRCint} – це ключ, котрий використовується тільки для захисту трафіку RRC з визначеним алгоритмом цілісності. K_{RRCint} отримують UE та eNB з ключа K_{eNB} ;
- K_{RRCenc} – це ключ, котрий використовується тільки для захисту трафіку RRC за допомогою визначеного алгоритму шифрування. K_{RRCenc} отримують UE та eNB з ключа K_{eNB} .

Розглянемо на рис. 2.15 процедуру автентифікації абонента.

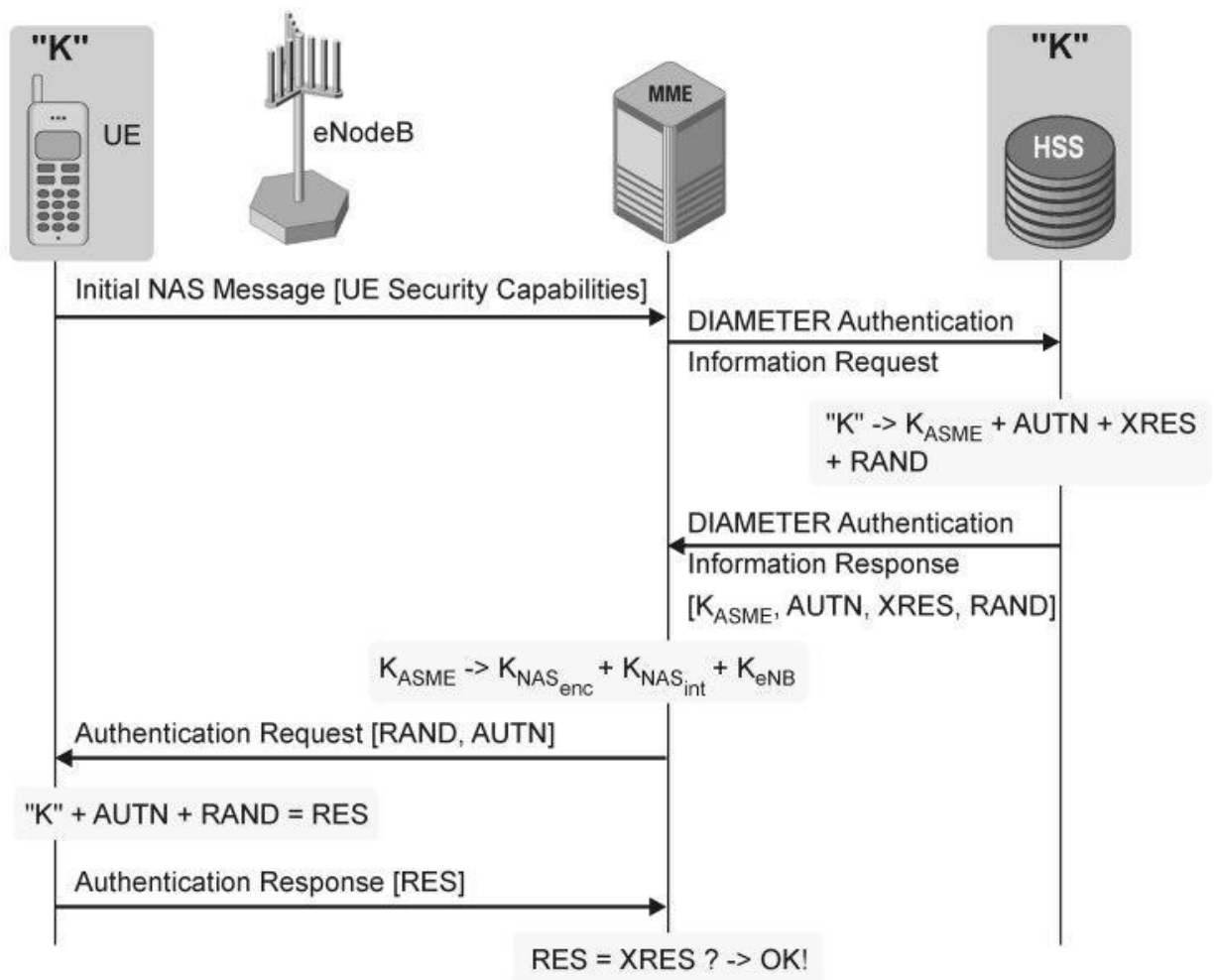


Рисунок 2.15 Процедура автентифікації абонента

Стартовим повідомленням, котре ініціює процедуру автентифікації мобільного пристрою є «Initial NAS Message». Воно надходить від UE до MME та містить інформацію про підтримувані мобільним пристроєм алгоритми шифрування і захисту цілісності.

Після того, як MME прийняв початкове повідомлення від UE, він зв'язується з домашнім сервером абонентів HSS по протоколу DIAMETER, щоб отримати новий вектор автентифікації, котрий містить ідентифікатор абонента. Сервер HSS зберігає секретний ключ мережі "K", який також міститься на USIM-карті, а ще він є унікальним для кожного оператора зв'язку. З ключа "K" та ідентифікатора абонента, HSS витягує три із чотирьох параметрів, а саме: ключ безпеки K_{ASME} , маркер автентифікації

(Authentication Token, AUTN) та маркер очікуваної відповіді (eXpected Response, XRES). Маркер випадкового числа (Random number, RAND) не є ідентифікатором і використовується лише для того, щоб підвищити рівень безпеки.

Сервер HSS відправляє до MME відповідь з новими маркерами автентифікації по протоколу DIAMETER. Коли блок управління мобільністю приймає дані чотири параметри, він формує ще три похідних від ключа K_{ASME} , а саме: K_{NASenc} (ключ шифрування NAS), K_{NASint} (ключ для захисту цілісності NAS) та K_{eNB} (ключ безпеки для eNB).

Після цього MME надсилає повідомлення із запитом до UE на автентифікацію «Authentication Request». Воно містить в собі випадкове число RAND та AUTN. Потім мобільний термінал повинен використати секретний ключ “K”, котрий міститься на USIM-карті, щоб згенерувати нове число на основі “K”, AUTN та RAND. Таким чином, UE формує відповідь автентифікації RES, що містить “K”, AUTN та RAND.

Коли мобільний термінал успішно згенерував відповідь RES, він надсилає відповідне повідомлення «Authentication Response» назад до MME. На останньому етапі процедури автентифікації блок управління мобільністю MME виконує порівняння параметрів RES та XRES, котре було вираховано раніше в домашньому сервері абонентів HSS. Якщо дані параметри мають однакове значення, то автентифікація абонента вважається успішно завершеною [34].

2.6 Висновки з розділу 2

В даному розділі було розглянуто принципи побудови еталонної архітектури ядра мережі LTE та інтерфейси взаємодії між різними підсистемами і вузлами. Детально описано функціонування системи IMS, як головного компоненту мережі для надання IP-сервісів оператора. Проаналізовано спосіб організації управління «дзвінками» в мережі LTE за

допомогою протоколу SIP. Також розглянуто метод управління доступом в мережу та принцип забезпечення безпеки абонентської інформації.

Еталонна архітектура EPC дозволяє перерозподілити функції мережевих елементів порівняно з мережами UMTS. Впровадження підсистеми IMS надає можливість організувати передачу голосового трафіку в мережах четвертого покоління, а також вводити нові види надання послуг. Для управління доступом в мережу застосовується глобальний унікальний тимчасовий ідентифікатор GUTI та функціональний рівень без доступу NAS, котрий забезпечує мобільність користувацьких терміналів, автентифікацію та встановлення сеансів зв'язку. Завдяки використанню нового методу автентифікації, тимчасових ідентифікаторів та надійних захищених протоколів, гарантується належний рівень безпеки в мережі.

3 СИСТЕМА УПРАВЛІННЯ МЕРЕЖЕЮ LTE

3.1 Управління мобільністю в мережі LTE

Мобільність – це важлива функція технології LTE, що забезпечує абонентам безперешкодне віддалене користування послугами мережі. Вузол MME є головним компонентом, котрий відповідає за управління мобільністю абонентів. Він з'єднаний по інтерфейсу S1-MME з великою кількістю базових станцій eNodeB, котрі згруповані в області відслідковування (Tracking Areas, TA) (рис. 3.1). Мобільний термінал може знаходитись в двох станах:

- в активному режимі «RRC-Connected», коли відбувається поточний обмін даними з мережею. Тоді місцезнаходження UE відомо до соти в якій він знаходиться;
- в режимі збереження енергії (очікування) «RRC-Idle», коли поточний обмін даними не відбувається. Місцезнаходження UE відомо мережі лише на рівні TA.

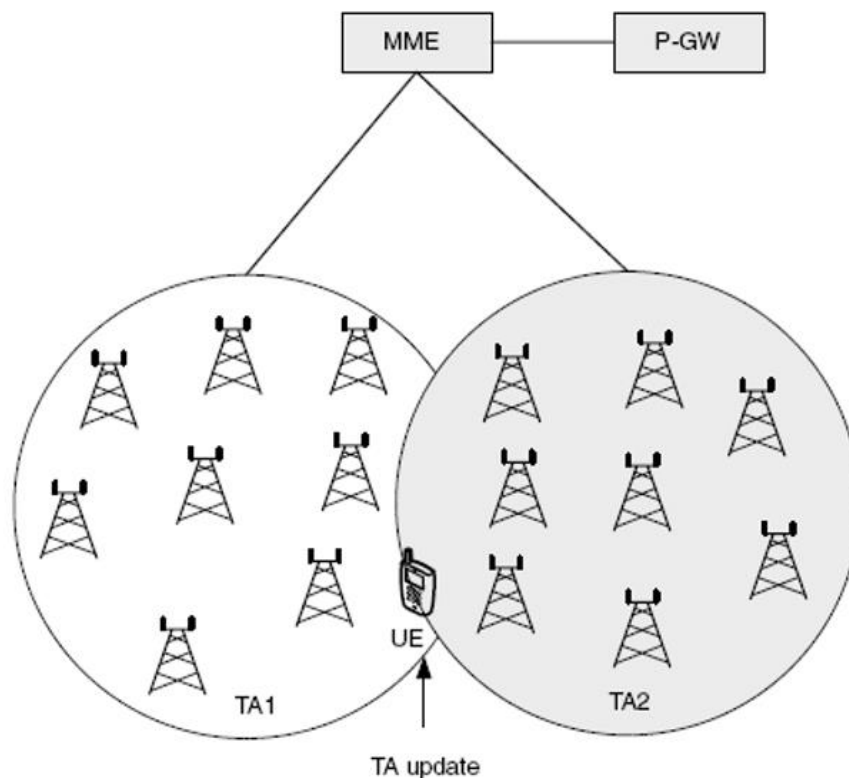


Рисунок 3.1 Область відслідковування TA

Область відслідковування TA – це логічна концепція області, в якій абонент може переміщуватись без додаткових оновлень місцезнаходження. Область TA складають eNodeB. Якщо потік даних направляється до мобільного терміналу, що знаходиться в стані «RRC-Idle», то MME повинен активувати його, щоб він міг прийняти дані. Така процедура має назву пейджинг (Paging). Таким чином, MME надсилає пейджингове повідомлення кожній базовій станції, що складають TA, в якій знаходиться UE. Потім eNodeB транслює відповідне повідомлення по радіоканалу, щоб активувати мобільний термінал. В свою чергу, він приймає його та переходить в активний режим «RRC-Connected» для прийняття даних. На рис. 3.2 зображено процедуру пейджингу.

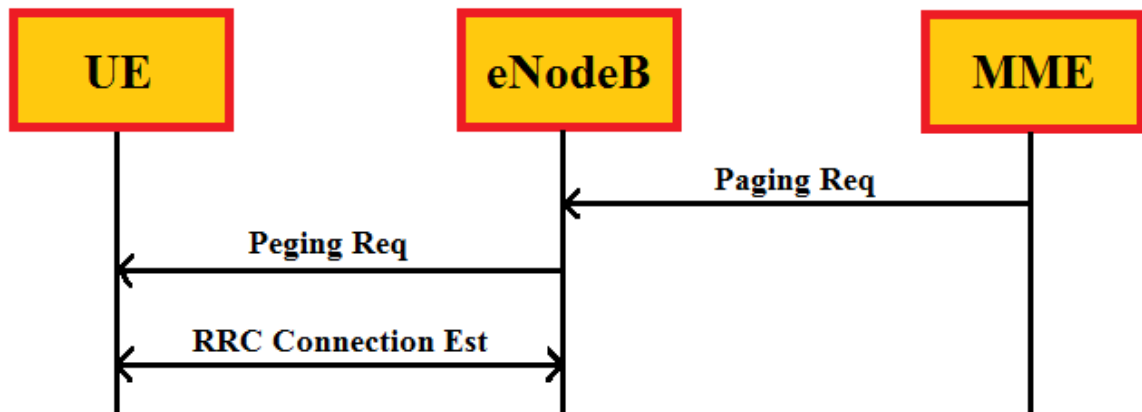


Рисунок 3.2 Процедура пейджингу

Блок управління мобільністю MME повинен мати оновлену інформацію про поточне місцезнаходження UE, що перебуває в стані очікування. Мобільний термінал стежить за ідентифікатором області відслідковування (Tracking Area Identity, TAI), в котрій він знаходиться на даний момент. У випадку переміщення UE в іншу TA, даний ідентифікатор змінюється. Тоді мобільний термінал ініціює процедуру оновлення області відслідковування (Tracking Area Update, TAU). Проте, дана процедура може виконуватись періодично, навіть коли він залишається в межах однієї TA. Якщо UE, перебуваючи в режимі очікування, не повідомив MME про своє поточне місцезнаходження, мережа не може визначити його стан. Таким

чином, мобільний термінал періодично надсилає запити на оновлення області відслідковування в MME, щоб повідомити мережу про спроможність приймати дані. В іншому випадку мережа вважає, що UE неактивний та не виконує процедуру пейджингу,

На рис. 3.3 зображено процедуру TAU.

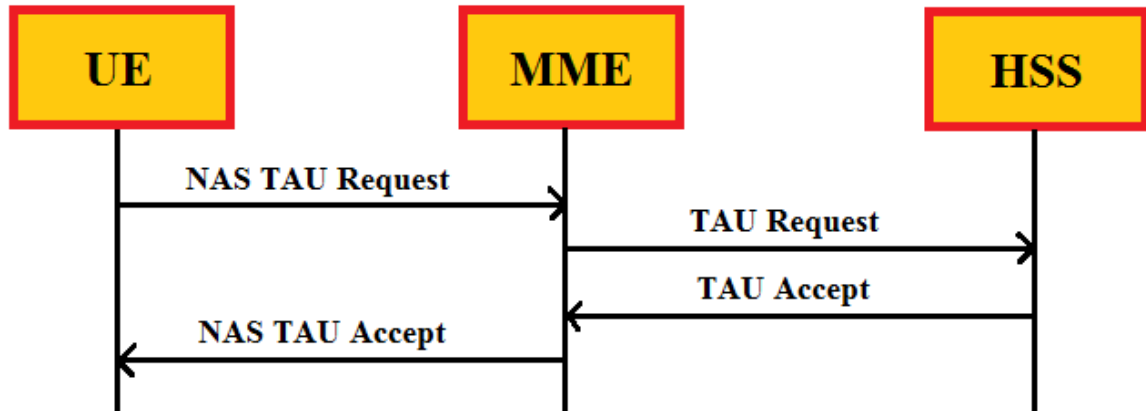


Рисунок 3.3 Процедура TAU

У мережі LTE, також для забезпечення мобільності, використовується процедура хендоверу. Завдяки їй відбувається «безшовна» передача обслуговування UE між вузлами мережі. Алгоритм функціонування хендоверу описаний і технічній специфікації TS 23.009 [35]. Дана процедура може поділятися на наступні типи:

- передача обслуговування в мережі радіодоступу, може застосовуватись для хендоверу між базовими станціями по інтерфейсу X2 під час переміщення абонентів. Проте, у випадку, коли інтерфейс X2 за певних причин недоступний, а вихідна базова станція та цільова знаходяться в зоні дії одного MME, то передача обслуговування проводиться по інтерфейсу S1;
- передача обслуговування між вузлами опорної мережі. Наприклад, якщо абонент, переміщаючись, покидає зону обслуговування одного MME, то виконується хендовер до іншого MME, котрий відповідає за цільові eNodeB. Також може бути здійснений хендовер між обслуговуючими шлюзами S-Gw;

- передача обслуговування між різними радіотехнологіями. Наприклад між E-UTRAN та UTRAN/GERAN. Перед здійсненням даного типу хендоверу, цільові вузли мережі виконують резервування необхідних ресурсів [36].

3.2 OAM-функціональність в мережі LTE

Операції, адміністрування та управління (Operation, Administration and Management, OAM) – це загальні процеси, операції, інструменти та стандарти пов’язані з експлуатацією, адмініструванням і управлінням будь якої телекомунікаційної системи. Операції включають в себе: автоматичний моніторинг всіх вузлів, виявлення і визначення відмов у роботі, сповіщення адміністратора. Адміністрування, в свою чергу, зазвичай включає: збір статистики продуктивності, даних для обліку, планування потужностей та підтримку надійності системи. До управління може відноситись: оновлення, виправлення, введення нових функцій, резервне копіювання та відновлення. Технічні принципи функціонування системи OAM розроблені міжнародним союзом електрозв’язку та описані в специфікації G.8013/Y.1731 [37].

В рамках концепції OAM функціонує система управління мережами зв’язку (Telecommunication Management Network, TMN), котра визначає принципи створення єдиної системи управління для мереж різних рівнів та масштабів. Також TMN забезпечує взаємодію різних типів операційних систем і телекомунікаційного обладнання з використанням стандартних протоколів та інтерфейсів. Мережа передачі даних в TMN призначена для організації зв’язку між мережевими елементами, апаратними системами та іншими пристроями, призначеними для управління. Дана система має ієрархічну структуру та включає наступні рівні:

- управління мережевими елементами, що забезпечує контроль, відображення параметрів функціонування та технічне обслуговування;

- управління мережею, що дозволяє єдиним чином здійснювати управління вузлами мережі;
- управління послугами (планування, облік та забезпечення якості обслуговування);
- адміністративне управління, що вирішує організаційні та фінансові питання.

На рис. 3.4 зображено ієрархію рівнів управління TMN.

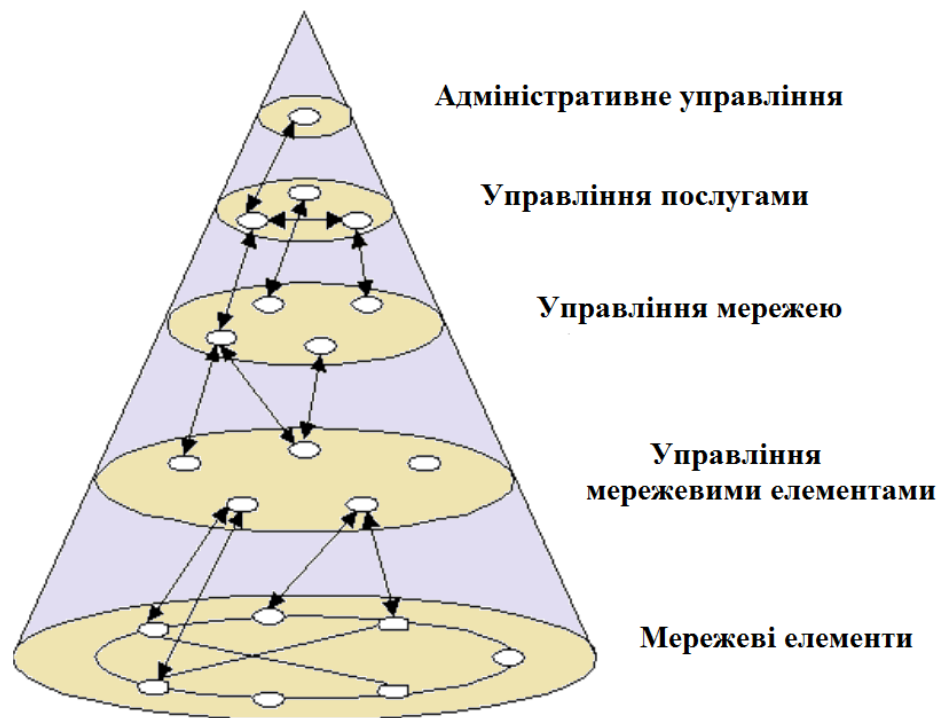


Рисунок 3.4 Ієрархія рівнів управління TMN

Організація управління мережею полягає у забезпеченні безвідмовного та узгодженого функціонування мережі зв'язку. Основними задачами при цьому є: моніторинг та контроль стану мережевих елементів, каналів транспортної мережі і взаємодій вузлів, а також управління роботою додатків та регулювання трафіку. Телекомунікаційні оператори використовують спеціальні системи підтримки операцій, котрі призначені для управління мережами та входять до складу системи управлінням зв'язку TMN. Головними функціями, що до них відносяться є:

- NRI (Network Resource Inventory), для технічного обліку мережевих

ресурсів;

- Fault Management, для збору та обробки аварійних повідомлень;
- Trouble Ticketing, для усунення різних несправностей;
- Fraud Management, для боротьби з шахраями;
- Performance Management, для управління продуктивністю.

OSS (Operation Support Subsystem) – це комп’ютерні системи обробки інформації, що призначені для управління телекомунікаційною мережею оператора. Як правило, вони надають функціональність, орієнтовану на мережу або мережеві операції. OSS допомагають проектувати, будувати, експлуатувати та підтримувати мережу. Головною перевагою даних систем є вміння обслуговувати одночасно велику кількість функціональних елементів, що можуть бути географічно віддаленими [38].

Оскільки мережі LTE для забезпечення високої ємності, відмінного покриття та якісного сервісу використовують значну кількість мережевих вузлів, то організація централізованого управління є пріоритетною задачею. Системи OSS зазвичай розробляються компаніями-виробниками мережевого обладнання та працюють лише в рамках одного бренду. Наприклад, компанія Ericsson для обладнання власного виробництва розробила спеціальну систему управління RC (Radio and Core), котра має відмінну від інших OSS архітектуру, інтерфейси та дизайн.

При впровадженні мереж четвертого покоління, оператори зв’язку зіткнулись з проблемою несумісності OSS для інших технологій мобільного зв’язку. Оскільки під час проектування мереж 2G та 3G використовувались інші постачальники обладнання, відповідно мали свої системи підтримки операцій. Поширеними виробниками є: Huawei, Ericsson, Nokia, ZTE та Alcatel-Lucent. Таким чином, наявність великої кількості систем управління для різного типу обладнання ускладнює основні принципи управління та моніторингу мережі. Також існує розподіл OSS між різними типами надання послуг. Наприклад, компанія Huawei застосовує різні системи управління для трансмісії (Mobile Backhaul Hierarchy, MBH), радіо частини (Mobile

BroadBand, MBB) та ядра мережі (Core Network System, CNS). Єдиним рішенням для спрощення управління та експлуатації мережі є зміна та модернізація обладнання мереж попереднього покоління. Загалом, наявність подібних рішень OSS дозволяють швидко розгорнути мережу та ефективно впроваджувати нові сервіси.

3.3 Висновки з розділу 3

В даному розділі було розглянуто поняття мобільності та забезпечення управління нею в мережі LTE. Також проаналізовано концепцію OAM, що дозволяє організувати систему керування мережею.

Використання таких процедур, як: пейджинг, оновлення області відслідковування TAU та хендовер, дає змогу здійснювати ефективно керування мобільністю абонентів. Організація управління мережею полягає у забезпеченні безвідмовного та узгодженого функціонування мережі зв'язку. В свою чергу, застосування системи підтримки операцій OSS дозволяє обслуговувати одночасно велику кількість функціональних елементів, що можуть бути географічно віддаленими.

ВИСНОВКИ

Відповідно до завдання на дипломну роботу, був здійснений огляд структури мережі четвертого покоління. Основною частиною роботи був аналіз архітектури та технічних принципів функціонування ядра EPC мобільного зв'язку LTE, а також побудови підсистеми IMS, як вагомого компоненту мережі для надання IP-сервісів оператором.

Вивчення та подальший розвиток ядра мережі LTE надасть багато переваг для телекомунікаційних компаній та, навіть, для звичайних користувачів. Тому, що подальша модернізація даного елементу мережі дозволяє вводити нові послуги, сервіси та покращувати якість зв'язку в цілому. Важливим фактом необхідності вивчення функціонування й побудови ядра EPC є те, що на основі нього розробляють мережі п'ятого покоління. Таким чином, опорна мережа буде залишатись практично незміненою. Саме тому, розробка способів поліпшити й надати нові функціональні можливості для опорного ядра мережі є досить пріоритетною задачею. Наразі існує достатня кількість джерел інформації, що дає змогу проаналізувати і з'ясувати методи та ефективність реалізації нових технологій при побудові ядра мережі.

Робота модернізованого ядра EPC засновано на функціонуванні IP-протоколу, тому методи передачі голосового трафіку з комутацією каналів, що використовуються в мережах попереднього покоління, не можуть бути застосовані. Завдяки взаємодії ядра EPC з мультимедійною підсистемою IMS з'являється можливість реалізувати встановлення голосових сесій в мережі LTE. Ядро EPC характеризується підвищеним рівнем безпеки, завдяки покращеному методу автентифікації, використанню тимчасових ідентифікаторів та функціонуванню безпечних протоколів сигналізації. Завдяки введенню критеріїв показників якості обслуговування, дана мережа може надавати різні види послуг за пріоритетами, наприклад, якщо передача голосу вимагає менші затримки пакетів, то пріоритет такого сервісу буде

вищим ніж передача інших сервісів, де більш важливим є показник втрати пакетів. Мобільність в мережі LTE забезпечується не лише в підсистемі радіодоступу, а й, безпосередньо, може управлятись модернізованим ядром EPC за допомогою спеціальних процедур таких, як: оновлення області відслідковування TAU, пейджингу та хендоверу між вузлами мережі. В свою чергу, концепція OAM-функціональності дозволяє організувати ефективне управління всією мережею. Таким чином швидке розгортання мережі даного типу не заважає керувати окремими вузлами.

Модернізоване ядро EPC – це елемент мережі, котрий безсумнівно потребує подальшого вивчення та розвитку. Його розробка є справжнім проривом в галузі мобільного зв'язку. Перехід до IP-архітектури надає безліч нових можливостей в наданні послуг та взаємодії з іншими підсистемами, а технічні принципи функціонування є основою для впровадження мереж наступного покоління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. РЫЖКОВ А.Е., Сиверс М.А., Воробьёв В.О., Гусаров А.С., Слышков А.С., Шуньков Р.В. Системы и сети радиодоступа – СПб: Линк, 2012. – 226 с.: ил.
2. 3GPP Specification: 21.201, Release 8. Technical Specifications and Technical Reports for an Evolved Packet System (EPS) based 3GPP system [Электронный ресурс].2008. Режим доступа: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=550>
3. Гельгор А.Л. Технология LTE мобильной передачи данных: учеб. пособие / Гельгор А.Л., Попов Е.А. — СПб.: Изд-во Политехн. ун-та, 2011. — 204 с.
4. С. Cox An Introduction to LTE – 2014 – John Wiley and Sons – 486 p.
5. F.Mohammed LTE BIBLE – 2018 – Nokia Networks – 306 p.
6. 3GPP Specification: 23.002. Network architecture [Электронный ресурс].2015. Режим доступа: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=728>
7. ETSI TS 124 302 v8.1.0 (2009-03). Universal Mobile Telecommunications Systems (UMTS); LTE; Access to the Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3 [Электронный ресурс].2009. Режим доступа: https://www.etsi.org/deliver/etsi_ts/124300_124399/124302/08.01.00_60/ts_124302_v080100p.pdf
8. 3GPP Specification: 23.122. Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode [Электронный ресурс].2015. Режим доступа: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=789>
9. 3GPP Specification: 43.022. Functions related to Mobile Station (MS) in idle mode and group receive mode [Электронный ресурс].2015. Режим доступа: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2664>

10. 3GPP Specification: 23.402. Architecture enhancements for non-3GPP accesses [Электронный ресурс].2015. Режим доступа: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=850>
11. 3GPP Specification: 33.401. 3GPP System Architecture Evolution (SAE); Security architecture [Электронный ресурс].2015. Режим доступа: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2296>
12. Тихвинский В.О., Тереньев С.В., Юрчук А.Б. Сети мобильной связи LTE: технологии и архитектура – М.: Эко-Трендз, 2010 – 284 с.:ил.
13. LTE Signaling, Troubleshooting and Optimisation, Ralf Kreher and Kasten Gaenger, 2011 – 282 p.
14. 3GPP Specification: 23.417. TISPA; IP Multimedia Subsystem (IMS); Functional architecture [Электронный ресурс].2015. Режим доступа: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=852>
15. 3GPP Specification: 23.517. TISPA; IP Multimedia Subsystem (IMS); Functional architecture [Электронный ресурс].2015. Режим доступа: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=859>
16. IMS architecture overview An overview of IMS architecture and related Accenture experiences. Università Federico II - Napoli, [Электронный ресурс].2017. Режим доступа: http://wpage.unina.it/rcanonic/didattica/at/lucidi_2007/AT_2006-07_IMS_Accenture.pdf
17. Voice over LTE (VoLTE) [Электронный ресурс].2020. Режим доступа: <https://itechinfo.ru/content/voice-over-lte-volte>
18. IMS VoLTE Architecture [Электронный ресурс].2020. Режим доступа: <http://www.3glteinfo.com/ims-volte-architecture/>
19. Сети связи следующего поколения (Лекция 14: IMS) [Электронный ресурс]. 2017. Режим доступа: <https://www.intuit.ru/studies/courses/1150/157/lecture/28726?page=3>

20. 3GPP Specification: 29.238. Interconnection Border Control Functions (IBCF) – Transition Gateway (TrGW) [Електронний ресурс].2015. Режим доступу: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1688>
21. IP Multimedia Subsystem (IMS) [Електронний ресурс].2013. Режим доступу: [http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:IP_Multimedia_Subsystem_\(IMS\)](http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:IP_Multimedia_Subsystem_(IMS))
22. SIP: Session Initiation Protocol [Електронний ресурс].2002. Режим доступу: <https://tools.ietf.org/html/rfc3261>
23. Гольдштейн Б.С., Зарубин А.А., Саморезов В.В. Протокол SIP: Справочник.: БХВ-Петербург, 2014. – 456 с.: ил.
24. Романов А.И., Верес Л.А., Явися В.С. Анализ Основных Протоколов Архитектуры IMS. Десята міжнародна науково-технічна конференція «Проблеми Телекомунікацій», с.155.
25. 3GPP Specification: 23.272. Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage2 [Електронний ресурс].2015. Режим доступу: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=835>
26. Ветошко І.П., Носков В.І. Технологія Передачі Голосу в Мережі LTE. Чотирнадцята міжнародна науково-технічна конференція «Проблеми Телекомунікацій»
27. 3GPP Specification: 23.216. Single Radio Voice Call Continuity (SRVCC); Stage 2 [Електронний ресурс].2015. Режим доступу: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=816>
28. E. Oquejiofor, P. Bazot, R. Huber, J. Kappel Developing SIP and IP Multimedia Subsystem (IMS) Applications [Електронний ресурс].2007. Режим доступу: <http://www.redbooks.ibm.com/redbooks/pdfs/sg247255.pdf>
29. 3GPP Specification: 31.102. Characteristics of the Universal Subscriber Identity Module (USIM) application [Електронний ресурс].2015. Режим доступу:

- <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1803>
30. 3GPP Specification: 24.301. Non-Access-Stratum protocol for Evolved Packet System (EPS) Stage 3 [Электронный ресурс].2015. Режим доступа: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1072>
 31. A. Elnashar, M. El-saidny, M. Sherif Design, Deployment and Performance of 4G – LTE Networks – 2014 – John Wiley and Sons – 609 p.
 32. V. Srinivasa Rao, Protokol Signaling Procedures in LTE, Radisys [Электронный ресурс].2011. Режим доступа: <https://go.radisys.com/rs/radisys/images/paper-lte-protocol-signaling.pdf>
 33. 3GPP Specification: 33.401. 3GPP System Architecture Evolution (SAE); Security architecture [Электронный ресурс].2016. Режим доступа: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2296>
 34. S. Bahrenburg LTE from A-Z - Technology and Concepts of the 4G 3GPP Standard - 2008 - INACON GmbH - 366 p.
 35. 3GPP Specification: 23.0009. Handover procedures [Электронный ресурс].2015. Режим доступа: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=732>
 36. M. Olsson, S. Sultana, S. Rommer, L. Frid, C. Mulligan. EPC and 4G Packet Networks.Driving the Mobile Broadband Revolution.2Ed.2013. [Электронный ресурс].2015. Режим доступа: https://www.academia.edu/27533347/EPC_and_4_G_Packet_Networks.Driving_the_Mobile_Broadband_Revolution.2Ed.2013.pdf
 37. Рекомендация МСЭ-Т G.8013/Y.1731(08/2015) Функции и механизмы эксплуатации, управления и технического обслуживания (ОАМ) для сетей на базе Ethernet. 97с.
 38. Управление транспортными сетями [Электронный ресурс].2016. Режим доступа: <https://siblec.ru/telekommunikatsii/integralnye-i-opticheskie-seti/2-transportnye-seti/2-7-upravlenie-transportnymi-setyami>